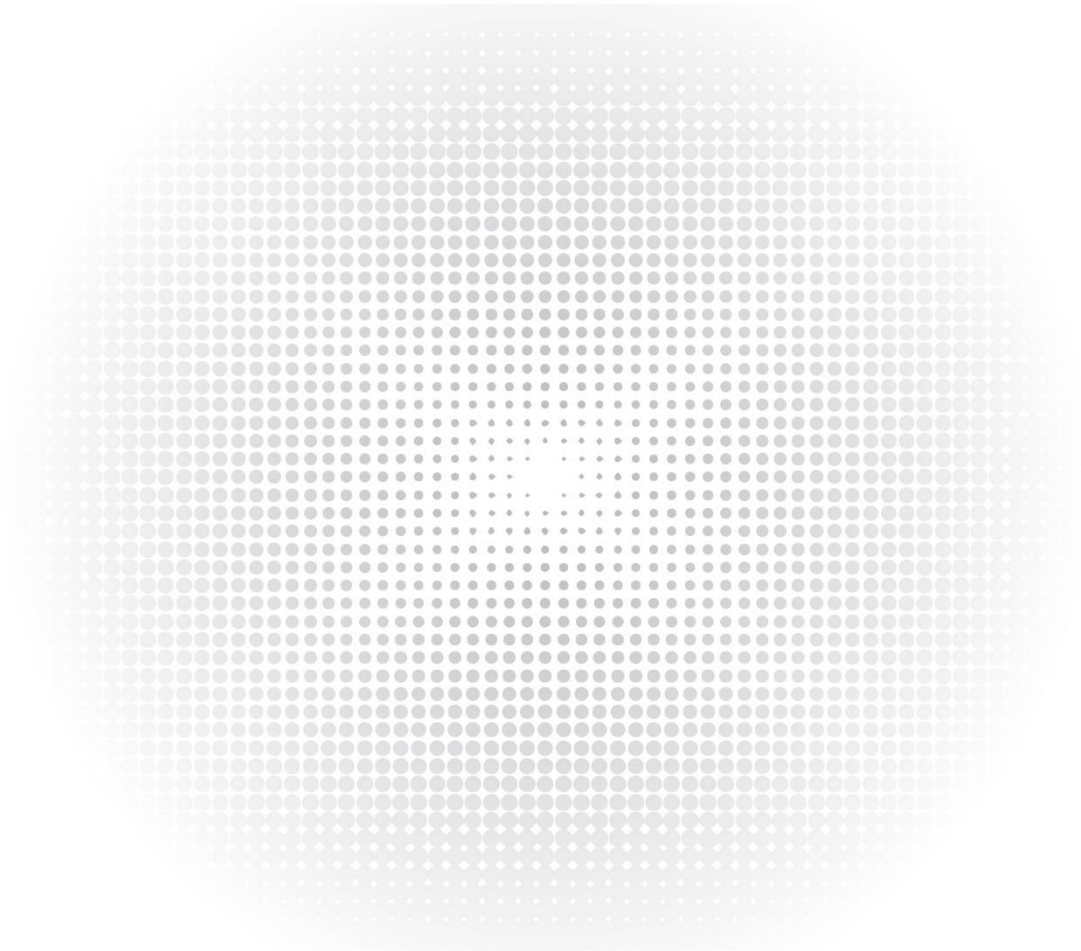
AC-1004 Wireless LAN Controller Configuration Guide

Models: AC-1004



Configuration Guide

Contents

Chapter 1 WLAN Basic Configuration 1
1 Configuring APMG 2
2 STAMG 65
3 STAMG Station Access Control List 119
4 CAPWAP 128
5 WBS 203
6 WLAN-WBS-FWD 286
7 DATA-PLANE 295
8 WLOG 297
9 ROAM 316
10 Interface Management 336
11 PoE 345
Chapter 2 WLAN RF 346
1RRM 347
2RRM 2.0 381
3 RF Schedule 390
4 Band Select 396
5 802.11kv 407
Chapter 3 Manual-WLAN Security 411
1RSNA 412
2 WIDS 448
3 CPP 532
4 NFPP 538
Chapter 4 WLAN QOS 633
1 WQOS 634
2 WMM 643
3VIP-FIRST 657
Chapter 5 WLAN networking 662
1 WDS 663
Chapter 6 Access Service 682
1Interface 683
2MAC Adress 720
3 VLAN 737
4 Super VLAN 752
5 MSTP 758
6 MAC VLAN 799
7 VLAN-Group 803
8 PPP 809
9 PPPOE-CLIENT 819
10 PPPoE-SERVER 835
Chapter 7 IP address and Application 847
1 IP address/server 848
2 ARP 879

3 DHCP 909
4 DNS 981
5 FTP-Server 989
6 FTP Client 998
7 TUNNEL 1005
8 Network Connectivity Test Tools 1021
9 TCP 1029
10 Software IPv4 Fast Forwarding 1047
11 TFTP-Server 1054
12 NAT 1060
Chapter 8 IP Routing 1084
1 protocol irrelevant 1085
2 NSM 1145
3 FPM 1160
4 ROUTE-DB 1173
Chapter 9 Security 1178
1 Web Authentication Configuration Commands 1179
2 AAA 1281
3 RADIUS 1323
4 802.1x 1354
6 Anti-Gateway ARP Spoofing 1419
7 Global IP+MAC binding 1421
8 DHCP Snooping 1422
9 IP Source Guard 1443
10 DNS SNOOPING 1451
11 IGMP Snooping 1457
12 ACL 1485
13 SCC 1538
14 PASSWORD-POLICY 1547
15 SSH 1553
16 CONTENT-AUDIT 1578
17 IPSEC-IKE 1674
18 VPDNs 1740
Chapter 10 System Configuration 1805
1 Command Line Interface 1806
2 Basic configuration management 1812
3 LINE 1863
4 RMON 1895
5 File System 1908
6 SNMP 1930
7 HTTP 1961
8 System log 1978
9 RLOG 2032
10 POLICE-LOG 2054

11 CWMP 2066
12 LEDs 2082
13 LICENSING 2085
14 USB 2098
15 PKG_MGMT 2102
16 SYS 2125
17 NTP 2158
18 SNTP 2171
19 TIME RANGE 2175
20 Abnormal alarm 2179
21 USER-TASK 2189
Chapter 11 Behavior Management 2196
1 layer23 2197
2 APP-IDENTIYF 2228
3 Global session limit 2280
4 FLOW-CONTROL 2302
5 FLOW-AUDIT 2329
6 CONTENT-AUDIT 2352

Chapter 1 WLAN Basic Configuration

1. Configuring APMG
2. Configuring STA Management
3. Configuring CAPWAP
4. Configuring WBS
5. Configuring WLAN WBS FWD
6. Configuring ETH-MNG
7. Configuring DATA-PLANE
8. Configuring WLOG
9. Configuring Roaming

1 Configuring APMG

1.1 ac-controller

Use this command to enter the AC configuration mode in the global configuration mode.

ac-controller

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 N/A

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】 N/A

【Configuration Example】 Enter the AC configuration mode。

```
AC-FS(config)# ac-controller
AC-FS(config-ac)#
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.2 acctrl-trap

In the AC configuration mode, use acctrl-trap to control the related trap switch on the AC.

acctrl-trap [acap-updown-ctrl | acap-joinfail-ctrl | acap-decryeroreport-ctrl | acap-imageupdt-ctrl | acap-timestamp-ctrl | acsta-oper-ctrl]

Restore to Default Configuration

no acctrl-trap [acap-updown-ctrl | acap-joinfail-ctrl | acap-decryeroreport-ctrl | acap-imageupdt-ctrl | acap-timestamp-ctrl | acsta-oper-ctrl]

【Parameter Description】

Parameter	Description
acap-updown-ctrl	Used to control CAPWAP tunnel up/down trap message sending.
acap-joinfail-ctrl	Used to control the sending of trap messages when AP fails to join the AC.
acap-decryeroreport-ctrl	Used to control the sending of trap messages that fail to decrypt the CAPWAP tunnel message.
acap-imageupdt-ctrl	Used to control the sending of trap information for the AP bin file upgrade.
acap-timestamp-ctrl	Used to control the sending of time synchronization trap information.

【Default Configuration】 off

【Command Mode】 AC configuration mode

【Default Level】 15

【Usage Guide】 Used to control the related trap switch on the AC.

【Configuration Example】 Configure AC to enable the sending of trap messages when APs fail to join AC.

```
AC-FS(config)#ac-controller
AC-FS(config-ac)#acctrl-trap acap-joinfail-ctrl
```

【Verification】 Through the show ac-config command, you can view the current switch status of various trap types.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.3 ac-name

In the AC configuration mode, configure the name of the AC through ac-name, which is convenient for users to identify。

ac-name ac-name

Restore to Default Configuration。

no ac-name

【Parameter Description】

Parameter	Description
ac-name	Configure the name of the AC. Up to 63 characters can be configured, and no spaces can be included.

【Default Configuration】 The default value of the AC name is the last six digits of the AC-FS_Ac_MAC address. For example, if the MAC address of the AC is 001a.a916.e7b8, the default name is AC-FS_Ac_16e7b8.

【Command Mode】 AC configuration mode

【Default Level】15

【Usage Guide】Configure different names for different ACs for user management.

【Configuration Example】 Configure the AC name as AC-FS-ac.

```
AC-FS(config-ac)# ac-name AC-FS-ac
```

【Verification】 Through the show ac-config command, you can view the current AC name.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.4 ap-auth

In the AP configuration mode, use the ap-auth command to configure the specified AP to perform access authentication. The methods that can be used are: AP-based serial number, AP-based password, AP-based certificate.

ap-auth { serial serial-string | password password | ac-cert ac-cert-name | ap-cert ap-cert-name }

Delete the related configuration through the no command.

no ap-auth { serial | password | ac-cert | ap-cert }

【Parameter Description】

Parameter	Description
serial-string	Specify the serial number of the AP.
password	Specify the AP access password.
ac-cert-name	Specify the name of the certificate file of the AC.
ap-cert-name	Specify the name of the AP's certificate file.

【Command Mode】 N/A

【Command Mode】 AP configuration mode

【Default Level】 15

【Usage Guide】 The authentication when the AP goes online is only valid when the AP is connected. If the AP is already online, the configuration will take effect when the AP goes online next time.

ap-auth serial Configuration in all mode is not supported, because the serial number of each AP is different.

The certificate file issued by ap-auth ap-cert will be saved as cert.crt on the AP, and the file name will not change.

【Configuration Example】 1: Configure AP1's authentication serial number.

```
AC-FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)# ap-config AP1
```

2: Delete AP1's certification serial number。

```
AC-FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)# ap-config AP1
```

【Verification】 show ap-config running shows the configuration of AP.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.5 ap-auth enable

In the AC configuration mode, configure the AP to enable the specified access authentication function through the ap-auth enable command. The methods that can be used are: based on the AP serial number, based on the AP password, and based on the AP certificate.

ap-auth [serial | password | certificate] enable

Turn off AP's access authentication.

no ap-auth [serial | password | certificate] enable

【Parameter Description】

Parameter	Description
serial	Authentication function based on AP access serial number.
password	Authentication function based on AP access password.
certificate	Authentication function based on AP certificate

【Default Configuration】 N/A

【Command Mode】 AC configuration mode

【Default Level】 15

【Usage Guide】N/A

【Configuration Example】 1: Turn on the authentication function based on AP access serial number.

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# ap-auth serial enable
```

2: Close the authentication function based on the AP access serial number

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# no ap-auth serial enable
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.6 ap-auth serial-update

In AC configuration mode, configure all online APs to update the authentication serial number through the ap-auth serial-update command.

ap-auth serial-update

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 N/A

【Command Mode】 AC configuration mode

【Default Level】 15

【Usage Guide】 This configuration will make all online APs use the serial number of the current AP as the authentication serial number configuration.

【Configuration Example】 Configure all online APs to renew the authentication serial number.

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# ap-auth serial-update
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.7 ap-backup group

In the AC configuration mode, create an AP backup group through the ap-backup group command.

ap-backup group name

Delete the AP backup group.

no ap-backup group name

【Parameter Description】

Parameter	Description
name	AP backup group name, default system reserved, that is, it is not allowed to configure default as the group name.

【Default Configuration】 Default Configuration, only the AP backup group named default exists on AC, and the backup function of this backup group does not take effect.

【Command Mode】 AC configuration mode

【Default Level】15

【Usage Guide】 When using the no command to delete an AP backup group, if there are AP members in the group, the APs in

the group are added to the default group, and the AP backup function of the default group will not take effect.

【Configuration Example】 1: Create an AP backup group named apbackup-test-group.

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# ap-backup group apbackup-test-group
```

2: Delete an AP backup group, and the group name is apbackup-test-group.

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# no ap-backup group apbackup-test-group
```

【Verification】 show ac-config ap-backup-group View the AP backup group created.

【Prompt Information】 -

【Common Mistake】 -

1.8 ap-backup-group

You can configure AP belonging to the specified AP backup group through the ap-backup group command in AP configuration mode.

ap-backup-group name [master]

Move the AP out of the AP backup group with the no prefix or cancel its primary AP role.

no ap-backup-group [name] [master]

【Parameter Description】

Parameter	Description
name	AP Backup group name.
master	Optional keyword that specifies the AP to the AP backup group as the primary AP.

【Default Configuration】 By default, AP do not join the default group, and the backup function of this backup group is not effective.

【Command Mode】 AP configuration mode

【Default Level】 15

【Usage Guide】 Before adding an AP to an AP backup group, the backup group needs to exist. The command plus the keyword "master" means to set the AP as the main AP of the AP backup group. If the AP group already has a master AP, the second AP with the role of the master AP is not allowed to join the AP backup group. If you need to change the AP For the master AP of the backup group, you need to cancel the previous master AP with the no command.

【Configuration Example】 1: Configure the AP to join the backup-test-group group and set it as the main AP of the group.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# ap-backup-group backup-test-group master
```

2: Set the AP that is already in the AP backup group to cancel the role of the main AP.

```
AC-FS(config-ap)# no ap-backup-group backup-test-group master
```

3: Configure AP to remove AP backup group.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# no ap-backup-group    AC-FS(config)# no ap-config AC-FS_AP
```

【Verification】 show ap-config running and show ac-config ap-backup-group to view the configuration.

【Prompt Information】 Connected ACs can deliver their own configurations to the AP.

【Common Mistake】 -

1.9 ap-config

The AP-config command can create an AP configuration, or enter the AP configuration mode.

ap-config ap-name

This command can remove an already existing AP group with the no prefix.

no ap-config ap-name

【Parameter Description】

Parameter	Description

ap-name	The name of the AP to be configure.

【Default Configuration】 N/A

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】 1. The user can enter the configuration mode of all APs through the command ap-config all, and the configuration in this mode will take effect for all APs associated with the AC. The priority of the configuration in the designated AP configuration mode is higher than that in the configuration mode of all APs. If there is a configuration in the ap-config ap-name configuration mode (that is, it is not the default configuration), then this configuration is preferred; otherwise, the configuration in the ap-config all configuration mode will be inherited.

2. The user can delete the specified AP configuration through the no ap-config ap-name command. If the corresponding AP of this configuration is already online, deleting the configuration will trigger the AP to go offline and go online.

The user can delete all offline AP configurations on the AC through the command no ap-config all.

【Configuration Example】 1: Create an AP configuration named AC-FS_AP.

```
AC-FS(config)#ap-config AC-FS_AP
You are going to config AP(AC-FS_AP), which is not on line now.
```

2: Configure to delete the AP configuration named AC-FS_AP.

```
AC-FS(config)# no ap-config AC-FS_AP
```

【Verification】 Through the show ap-config running command, you can view all AP configurations.

【Prompt Information】 -

【Common Mistake】 -

1.10 ap-group

All AP joining AC will belong to and only belong to a specific AP group at a time. All newly added AP belong to the default AP group: default. You can use ap-group to create a new AP group, or enter the configuration mode of an AP group. If an AP group is created, it will enter the configuration mode of the AP group after creation.

ap-group ap-group-name

This command can delete an existing AP group by using the no prefix.

no ap-group ap-group-name

【Parameter Description】

Parameter	Description
ap-group-name	The name of the AP group can be up to 63 bytes in length without any spaces.

【Default Configuration】 By default, a default AP group (group name: default) will be created automatically after the system is started, and this group cannot be created or deleted.

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】 When deleting an AP group, the APs belonging to the AP group will automatically switch to the default group.

【Configuration Example】 1: Create an AP group and the AP group name is test-group.

```
AC-FS(config)# ap-group test-group
AC-FS(config-ap-group)#
```

2: Delete an AP group, the AP group is named test-group.

```
AC-FS(config)#no ap-group test-group
```

3: Enter an AP group, enter the default AP group in the example, the AP group name is default

```
AC-FS(config)# ap-group default
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.11 ap-group（ap configuration mode）

All AP joining AC will belong to and only belong to a specific AP group at a time. All newly added APs belong to the default AP group: default. You can configure the AP to belong to the specified AP group by using the ap-group command in the AP configuration mode.

ap-group ap-group-name

The AP is restored to the default group by using the no prefix.

no ap-group

【Parameter Description】

Parameter	Description
ap-group-name	AP group name

【Command Mode】 AP configuration mode

【Default Level】 15

【Usage Guide】 When an AP group is deleted, the APs belonging to the AP group will automatically switch to the default group.

【Configuration Example】 1: Configure AP to join test-group group.

```
AC-FS(config)# ap-group test-group Ruieji(config-ap-group)#
AC-FS(config)# ap-config AP0001
```

2: Configure AP to revert to default group.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# no ap-group test-group
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.12 ap-mac

In AP configuration mode, the MAC address of the AP can be bound by ap-mac.

ap-mac ap-mac

The no command removes the ap-mac binding.

no ap-mac

【Parameter Description】

Parameter	Description
ap-mac	The MAC address of the AP.

【Default Configuration】 None

【Command Mode】 AP configuration mode

【Default Level】15

【Usage Guide】 1. In AP configuration mode, use the ap-mac command to configure the bound MAC address for the AP, so that the AP configuration can only take effect on the AP with the bound MAC address.

2. Generally, the AP goes online to determine which configuration the AP uses by matching the AP name with the AP configuration name. MAC address binding is a stronger binding relationship than name matching, and its priority is higher than name matching. Therefore, as long as the MAC address bound to the AP configuration is consistent with the AP's MAC address, the AP will use this configuration when it goes online.

3. MAC address binding automatically: If the corresponding AP configuration is not configured with MAC address binding, when the corresponding AP goes online, it will automatically

MAC address binding, the binding relationship is still valid when the AP goes offline, that is, the configuration will be automatically generated after the AP goes online.

4. MAC address binding is also used for the bind-ap-mac access control function of AP access control. For details, see bind-ap-mac

configuration description.

5. Can only specify MAC address binding for offline AP configuration. If the corresponding AP is already online, it cannot be configured to specify MAC address binding.

【Configuration Example】 1: The AMC address bound to ap test is 00ff.ffff.1111.

```
AC-FS(config)# ap-config test
AC-FS(config-ap)# ap-mac 00ff.ffff.1111
```

【Verification】 Use the show ap-config running command to view the ap-mac configuration of the current AP.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.13 ap-mode

On the AP, you can switch the mode of the AP through ap-mode.

ap-mode { fit | fat [dhcp] | macc }

【Parameter Description】

Parameter	Description
fit	Switch to fit AP mode.
fat	Switch to fat AP mode.
dhcp	The ap-mode fat command carries this option (ie ap-mode fat dhcp), after the AP is configured to switch to fat AP mode, the AP will use DHCP to obtain the IP address by default; otherwise, after the AP is configured to switch to fat AP mode, the AP will use by default Static IP address.
macc	Switch to macc mode.

【Default Configuration】 None

【Command Mode】 AP Global configuration mode

【Default Level】 15

【Usage Guide】 After the mode switch, restart is required to ensure the consistency of the configuration.

The default IP address of the back-end wired interface of the fat AP (wired interface connected to POE switching equipment) and the thin AP is 192.168.110.1/255.255.255.0, The default IP address of the front-end wired network interface (Ethernet port provided on the front of the product) of the fat AP is 192.168.111.1/255.255.255.0.

If ap-mode fat dhcp is configured, when the AP is switched to fat AP mode, the default is to obtain the address by DHCP. At the same time, after the AP is restarted, if there is no related configuration, the default is to obtain the address by DHCP. In addition, you need to pay attention to two things point:

If the AP is configured with ap-mode fat dhcp, only the back-end wired interface defaults to using DHCP, and the front-end wired network interface defaults to using a static address.

Fit/fat/fat dhcp/macc four modes. Switching between the two modes will delete the current configuration and reboot. After rebooting, the AP loads the default configuration of the corresponding mode.

In fit mode, the default login password in user mode is AC-FS, and the default login password in privileged mode is apdebug.

In the three modes of fat/fat dhcp/macc, the user mode default login password is admin, and the privileged mode has no default login password.

【Configuration Example】 1: Switch AP to fit mode.

```
AC-FS(config)# ap-mode fit
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 Only AP support

1.14 ap-name

AC device is in AP configuration mode, or AP device configuration mode, configure the name of AP through ap-name.

ap-name ap-name

Delete the AP name configuration.

no ap-name

【Parameter Description】

Parameter	Description
ap-name	Configure the name of the AP. Up to 63 characters can be configured, and no spaces can be included.

【Default Configuration】 None

【Command Mode】 AP configuration mode

【Default Level】 15

【Usage Guide】 Configuration on AC:

If the corresponding AP is online, the AP name configuration will take effect immediately. At the same time, the AP configuration mode name (ie, the character string after ap-config) will be replaced with the new name immediately.

If the corresponding AP is offline, the configuration of the AP name will take effect when the corresponding AP is online, and the name of the AP configuration mode will remain the original name until the corresponding AP is online and the configuration takes effect.

After the AP name is configured, you can continue to configure the AP without exiting the AP configuration mode.

If the corresponding AP is online, the no command is not supported.

If the corresponding AP is offline, the no command will clear the AP name configuration that is not valid.

If the new name has been used, the configuration is unsuccessful.

Up to 63 characters can be configured, no spaces are allowed.

Cannot configure the AP name as "all" and "AP".

It should be avoided to configure the same new name for different offline APs in the configuration. If different offline APs are configured with the same new name, the AP that went online first will take effect with the new name, and the APs that go online will retain the original name and cannot use the new name.

Configuration on AP:

If the AP is online, after the name is configured, the tunnel is disconnected and the connection is re-established. If the AP's name is not revised on the AC, that is, the AC is the default name, then the revised name of the AP is used to access, otherwise it is configured on the AC the name prevails.

If the AP is not online, the AP connects to the AC. If there is no offline configuration on the AC, then the AP configuration prevails. If the AC has an offline configuration, then the AC configuration prevails.

If the name configured on the AP conflicts with the name configured on other APs on the AC, the AP access is unsuccessful.

Up to 63 characters can be configured, and no spaces are allowed.

The AP name cannot be configured as "all".

【Configuration Example】 1: The new name of AP0001 is AP_NEW on the AC.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# ap-name AP_NEW
```

2: The name configured on the AP is AP_TEST.

```
AC-FS(config)# ap-name AP_ TEST
```

【Verification】 1: On the AC

View the current AP configuration through the command show ap-config running.

Through the command show ap-config summary, you can check whether the name of the online AP is the new name of the configuration.

2: On the AP

View the current AP name configuration through the command show running.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC and Fit AP support

1.15 ap-priority

In the AC configuration mode, the ap-priority command is used to enable/disable the support for the AP. Failover priority.

ap-priority { enable | disable }

【Parameter Description】

Parameter	Description
enable	Enable support for AP's Failover priority.
disable	Disable the support for AP's Failover priority.

【Default Configuration】 Default off

【Command Mode】 AC configuration mode

【Default Level】 15

【Usage Guide】 -

【Configuration Example】 1: AP0001 is connected to AC1. Configure the Failover priority of the AP (AP0001) to 3, and turn on the AC1 Failover priority function support switch.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# priority 3
AC-FS(config-ap)# exit
AC-FS(config)# ac-controller
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.16 backup-controller-primary

Configure AP's fourth option AC.

backup-controller-primary ac-name { ip-address } [switch-back]

Delete the 4th choice AC configuration.

no backup-controller-primary

【Parameter Description】

Parameter	Description
ac-name	Configure the name of the AC. Up to 63 characters can be configured, and no spaces can be included.
ip-address	The format is: A.B.C.D. The IP address of the AC.
switch-back	The switchback function is configured, and the switchback is not by default.

【Default Configuration】 N/A

【Command Mode】 AP configuration mode/all AP configuration mode

【Default Level】 15

【Usage Guide】Configure the AP's redundant AC with the above command. primary-base is the preferred AC, secondary-base is the second option AC, tertiary-base chooses AC for the third choice, backup-controller-primary selects AC for the fourth, backup-controller-secondary is the fifth option AC, backup-controller-tertiary is the sixth option AC.

The above command supports ap-config ap-name and ap-config all configuration modes at the same time, according to ap-config ap-name has priority higher than ap-config all to take effect.

【Configuration Example】 Set the fourth choice of AP ap1, AC to ac1, and the IP address of ac1 to 192.168.1.4.

```
AC-FS#config terminal
AC-FS(config)#ap-config ap1
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.17 backup-controller-secondary

Configure the fifth choice AC for AP.

backup-controller-secondary ac-name { ip-address } [switch-back]

Delete fifth choice AC configuration.

no backup-controller-secondary

【Parameter Description】

Parameter	Description
ac-name	Configure the name of the AC. Up to 63 characters can be configured without spaces.
ip-address	The format is: A.B.C.D. The ip address of the AC.
switch-back	Configure the switchback function, and no switchback by default.

【Default Configuration】 N/A

【Command Mode】 AP configuration mode/all AP configuration mode

【Default Level】 15

【Usage Guide】 Configure the AP's redundant AC with the above command. primary-base is the preferred AC, secondary-base is the second option AC, tertiary-base is the third choice AC, backup-controller-primary is the fourth choice AC, backup-controller-secondary is the fifth choice AC, backup-

The above command supports both ap-config ap-name and ap-config all configuration modes, according to ap-config ap-name has priority higher than ap-config all to take effect.

【Configuration Example】 Set the fifth choice of AP ap1, AC to ac1, and the IP address of ac1 to 192.168.1.4

```
AC-FS#config terminal AC-FS(config)#ap-config ap1
AC-FS(config-ap)#backup-controller-secondary ac1 192.168.1.4
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.18 backup-controller-tertiary

The sixth choice for configuring AP is AC.

backup-controller-tertiary ac-name { ip-address } [switch-back]

Delete the sixth selection AC configuration.

no backup-controller-tertiary

【Parameter Description】

Parameter	Description
ac-name	Configure the name of the AC. Up to 63 characters can be configured without spaces.

ip-address	The format is: A.B.C.D. The ip address of the AC.
switch-back	Configure the switchback function, and no switchback by default.

【Default Configuration】 N/A

【Command Mode】 AP configuration mode/all AP configuration mode

【Default Level】 15

【Usage Guide】 Configure the AP's redundant AC through the above command. primary-base is the preferred AC, secondary-base is the second option AC, tertiary-base is the third choice AC, backup-controller-primary is the fourth choice AC, backup-controller-secondary is the fifth choice AC, backup-controller-tertiary is the sixth choice AC.

The above command supports both ap-config ap-name and ap-config all configuration modes, According to ap-config, ap-name takes effect higher than ap-config all.

【Configuration Example】 Set the sixth choice AC of AP ap1 to ac1, and the IP address of ac1 to 192.168.1.4

```
AC-FS#config terminal
AC-FS(config)#ap-config ap1
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.19 bind-ap-mac

Configure to enable AP compliance check through the command bind-ap-mac.

bind-ap-mac

Close AP compliance check.

no bind-ap-mac

【Parameter Description】 -

【Default Configuration】 Off

【Command Mode】 AC configuration mode

【Default Level】15

【Usage Guide】Use the bind-ap-mac command in AC configuration mode to enable AP compliance check.

When the bind-ap-mac function is turned on, all the automatically bound MAC addresses of all online APs will be converted to formal MAC address binding, and will not be automatically cleared when the AP is offline.

You can also configure the MAC address binding of a single AP configuration through the ap-mac X.Y.Z command in AP configuration mode.

【Configuration Example】 1: Configure to enable AP compliance check.

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# bind-ap-mac
```

2: Configure to turn off AP compliance check.

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# no bind-ap-mac
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.20 credential

Users can configure AP username and password through credential.

credential user-name password

Cancel this configuration.

no credential

【Parameter Description】

Parameter	Description
user-name	The username to be used on the AP, no spaces allowed.
password	The password to be used on the AP, no spaces allowed.

【Default Configuration】 There is no Default Configuration for this command

【Command Mode】 AP configuration mode or AP group configuration mode

【Default Level】 15

【Usage Guide】 N/A

【Configuration Example】 1: The user name for configuring AP0001 is: first-ap, and the password is: 123456.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# credential first-ap 123456
```

2: Configure the user name of all APs under the AP group (Default): first-ap and password: 123456.

```
AC-FS(config)# ap-group default
AC-FS(config-ap-group)# credential first-ap 123456
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.21 enable-broad-ssid

WLAN configuration mode, enable-broad-ssid to enable SSID broadcasting.

enable-broad-ssid

Disable SSID broadcast.

no enable-broad-ssid

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 By default, it is enable.

【Command Mode】 WLAN configuration mode

【Default Level】 15

【Usage Guide】 Configure the Suppress SSID information of the WLAN. The configuration takes effect only before the WLAN application. If the WLAN has been deployed, this command will cause the user currently associated with the WLAN to go offline.

【Configuration Example】 1: Enable SSID broadcasting on this WLAN.

```
AC-FS(config-wlan)#enable-broad-ssid
```

2: Disable SSID broadcasting on this WLAN

```
AC-FS(config-wlan)#no enable-broad-ssid
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.22 factory-reset

Use the factory-reset command to configure the specified AP to restore the factory settings. This operation will cause the AP to reset.

factory-reset ap-name

【Parameter Description】

Parameter	Description
ap-name	AP name to restore factory settings

【Default Configuration】 None

【Command Mode】 AC configuration mode

【Default Level】 15

【Usage Guide】 The configuration restores the factory settings of the specified AP. This operation will cause the AP to reset.

【Configuration Example】 Configure AP0001 to restore factory settings.

```
AC-FS(config-ac)# factory-reset AP0001
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.23 interface-mapping

Mapping wlan-vlan or wlan-vlan-group through interface-mapping in AP group configuration mode (The mapping in the description of this command refers to wlan-vlan or wlan-vlan-group mapping) Map to the radio of all APs in the AP group. Through this mapping, wlan related configuration information can be applied to the specified radio.

interface-mapping wlan-id [vlan-id I group vlan-group-id] [radio {radio-id | [802.11b | 802.11a]}] [ap-wlan-id ap-wlan-id]

Delete the related mapping configuration.

no interface-mapping wlan-id [vlan-id I group vlan-group-id] [radio {radio-id | [802.11b | 802.11a]}] [ap-wlan-id ap-wlan-id]

【Parameter Description】

Parameter	Description
wlan-id	The ID of the wlan to be mapped, the wlan must have been created, and the value range is 1~4094.
vlan-id	The ID of the VLAN to be mapped, the value range is 1~4094.
vlan-group-id	The ID of the vlan-group to be mapped, the value range is 1~128.
Radio-id	To apply the radio of the AP whose mapping is specified, the value range is reserved 1~96 defined by the standard. If the radio-id parameter is not specified, the mapping will be applied to all radios of all APs in the AP group.
802.11b	The mapping will be applied to the 2.4G radios of all APs in the AP group.
802.11a	The mapping will be applied to the 5.8G radios of all APs in the AP group.
ap-wlan-id	Specify the wlan-id used by wlan-id on ap in interface-mapping, the value range is: 1~64. If the ap-wlan-id parameter is not specified, the mapping will automatically select a free ap-wlan-id to use.

【Default Configuration】 N/A

【Command Mode】 AP group configuration mode

【Default Level】 15

【Usage Guide】 When the WLAN forwarding mode is local forwarding, When the vlan-id configured by this command or the vlan-id assigned to the STA in the vlan-group mode is the same as the vlan-id specified by the ap-vlan command, The real VLAN of the STA will be determined by the AP's access switch instead of the VLAN configured by this command or the VLAN assigned in the vlan-group mode. fIn particular, since the default vlan-id of ap-vlan is 1, that is, when ap-vlan is not configured, if the vlan-id configured by this command is 1, then the VLAN of the STA under local forwarding will be determined by the access switch. Since the VLAN of the AP is determined by the access switch,When the VLAN of the STA is the same as the Native VLAN of the access switch, it is also required that ap-vlan is the same as the Native VLAN of the access switch,otherwise STA will not be able to communicate(The uplink requirements and AP belong to different VLANs, and the downlink requires the same VLAN, which conflicts).

【Configuration Example】1: Create vlan 2, create a wlan with ID 4094, and apply the mapping of wlan4094-vlan2 to radio 1 of all APs in the default AP group

```
AC-FS(config)#vlan 2
AC-FS(config)#wlan-config   4094   pro-4094   ssid-4094
AC-FS(config-wlan)#exit
AC-FS(config)#ap-group default
```

2: Create a wlan with ID 4094, and apply the mapping of wlan4094-vlan2 to radio 1 of all APs in the default AP group.

```
AC-FS(config)#vlan-group 3
AC-FS(config)#wlan-config   4094   pro-4094   ssid-4094
AC-FS(config-wlan)#exit
AC-FS(config)#ap-group default
```

3: Enter the default AP group and delete the configured wlan4094-vlan2 mapping.

```
AC-FS(config)# ap-group default
FS(config-ap-group)# no interface-mapping 4094 2 radio 1
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.24 logging on

Configure AP to turn on system log display.

logging on

Use the no option of this command to prohibit AP from displaying system log information.

no logging on

【Parameter Description】 -

【Default Configuration】 Allow system log to be displayed

【Command Mode】 AP configuration mode or all AP configuration mode

【Default Level】 15

【Usage Guide】 N/A

【Configuration Example】 1: Configure AP to forbid printing system log

```
AC-FS(config-ap)#no logging on
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.25 logging server

Configure the AP to record system log information to the execution server.

logging server ip-address [udp-port num]

Use the no option of this command to delete the specified server.

no logging server ip-address

【Parameter Description】

Parameter	Description
ip-address	IP address of the host receiving the log information.
num	Port number of the host that receives the log information (optional).

【Default Configuration】 N/A

【Command Mode】 AP configuration mode/all AP configuration mode

【Default Level】 15

【Usage Guide】 The user can configure up to 5 log server addresses, and the log information will be sent to all configured log servers at the same time.

【Configuration Example】 1: Configure the address of the log server as 1.1.1.1

```
AC-FS(config-ap)# logging server 1.1.1.1
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.26 nassid

Configure WLAN user or AC access location number.

nas-id nas-id

Use the no option of this command to restore to Default Configuration.

no nas-id

【Parameter Description】

Parameter	Description
nas-id	Access site number, contains 32 characters, no spaces.

【Default Configuration】 WLAN user access code default empty string.

AC access location code Default AC MAC address dotted form string.

【Command Mode】 WLAN configuration mode or AC configuration mode

【Default Level】 15

【Usage Guide】 N/A

【Configuration Example】 1: Configure the WLAN access user site number as 0000059159100460.

```
AC-FS(config-wlan)# nas-id 0000059159100460
```

2: Restore the WLAN access user site number to the default value.

```
AC-FS(config-wlan)# no nas-id
```

3: Configure the AC access point number as 123456789.

```
AC-FS(config-ac)#nas-id 123456789
```

4: Restore the AC access point number to the default value.

```
AC-FS(config-ac)# no nas-id
```

【Verification】 View the specified WLAN user access code through the show wlan-config cb command.

```
AC-FS(config)#show wlan-config cb 1
WLAN ID    1
SSID..... 1-leichen-test-wlan
Profile
MAC Mode Local
Tunnel Mode.....  802.3 Tunnel
Suppress SSID     Disable
Sta-limit     0
```

View the AC access code through the show ac-config command.

```
AC-FS(config)# show ac-config
AC Configuration info:
max_wtp         : 10
 sta_limit         : 81920
license wtp max : 2560 license sta max : 81920
serial auth           : Disable
password auth : Disable certificate auth : Disable
```

```
ac_name         : AC-FS_Ac_050607 ac location         : AC-FS_COM
AC State info:    sta_num         : 1 act_wtp         : 1
localIpAddr         10.10.10.10
localIpAddr6       : : :
used wtp    1.0(0 four 1 normal 0 half)
remain wtp             : 2 four 9 normal 18 half HW Ver   1.00
SW Ver                 : AC_RGOS 11.1(5)B6, Release(02193103)
```

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.27 offline-ssid

After configuring offline-ssid, before the thin AP starts up and has not established the capwap tunnel or after the capwap tunnel of the AP is disconnected, the AP releases the signal to provide the WLAN access service function.

offline-ssid ssid [hide]

Revert to Default Configuration

no offline-ssid

【Parameter Description】

Parameter	Description
ssid	Provide wireless signals for WLAN access.
hide	Set the released signal to not broadcast.

【Default Configuration】 N/A

【Command Mode】 AP configuration mode, AP group configuration mode, all AP configuration mode

【Default Level】 15

【Usage Guide】The AP device restarts and the configuration will be saved.

Chinese signal is not supported

When ript is configured, the tunnel is disconnected and the signal is not released.

【Configuration Example】 1: Set the default SSID of AP1 to my-def-ssid.

```
AC-FS(config)#ap-config AP1

AC-FS(config-ap)#offline-ssid my-def-ssid
```

【Verification】 show ap-config running

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

1.28 primary-base

Configure AP's preferred AC.

primary-base ac-name { ip-address }

Delete the preferred AC configuration.

no primary-base

【Parameter Description】

parameter	Description
ac-name	Configure the name of the AC. Up to 63 characters can be configured without spaces.
ip-address	The format is: A.B.C.D. The ip address of the AC.

【Default Configuration】 N/A

【Command Mode】 AP configuration mode/all AP configuration mode

【Default Level】 15

【Usage Guide】 Configure the AP's redundant AC through the above command. primary-base is the preferred AC, secondary-base is the second option AC, tertiary-base is the third choice AC, backup-controller-primary is the fourth choice AC, backup-controller-secondary is the fifth choice AC, backup-controller-tertiary is the sixth choice AC.

The above command supports both ap-config ap-name and ap-config all configuration modes. According to ap-config, ap-name has a higher priority than ap-config all to take effect.

【Configuration Example】 Set the preferred AC of AP ap1 to ac1, and the IP address of ac1 to 192.168.1.1.

```
AC-FS#config          terminal
AC-FS(config)#ap-config ap1
AC-FS(config-ap)#primary-base ac1 192.168.1.1
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.29 priority

This command is used to set the AP's Failover priority, after enabling the AP's Failover priority support on the AC, AC can accept AP access according to the priority order of AP.

priority priority-value

【Parameter Description】

Parameter	Description
priority-value	Configure AP's Failover priority. The allowed values are 1~4, where 1 is the lowest priority and 4 is the highest priority.

【Default Configuration】 The default priority of AP's Failover is 1.

【Command Mode】 AP configuration mode

【Default Level】 15

【Usage Guide】 Configure device Failover priority. 1 has the lowest priority, 4 has the highest priority. The order in which APs are added to the AC configured here (that is, the priority of APs), After the configuration, it will be saved in the AP, and it will take effect when the AP associates next time.

【Configuration Example】 1: Configure the Failover priority of the AP group ap group to 3.

```
AC-FS#config terminal AC-FS(config)#ap-config ap001
AC-FS(config-ap)#priority 3
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.30 reload at

You can use the reload at command in the AP configuration mode to configure the designated AP to restart regularly every day.

reload at time

Delete the daily restart configuration.

no reload at

【Parameter Description】

Parameter	Description
time	The time point defined in the form of HH: mm: SS for regular restart every day.

【Default Configuration】 None

【Command Mode】 AP configuration mode

【Default Level】 15

【Usage Guide】 None

【Configuration Example】 1: Configure AC-FS-AP1 to restart regularly at 1: 00: 00 every day.

```
AC-FS(config)#ap-config AC-FS-AP1
AC-FS(config-ap)#reload at 1: 00: 00
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.31 reset

You can use the reset command to configure all AP or specify AP to reset in the AC configuration mode.

reset { all | single ap-name }

【Parameter Description】

Parameter	Description
all	Reset all AP.
Reset all AP	Reset the specified AP.

【Default Configuration】 N/A

【Command Mode】 AC configuration mode

【Default Level】 15

【Usage Guide】 N/A

【Configuration Example】 1: Configure all AP reset.

```
AC-FS(config-ac)# reset all
```

2: Reset the AP named AP0001.

```
AC-FS(config-ac)# reset AP0001
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.32 secondary-base

Configure AP's second option AC.

secondary-base ac-name { ip-address } [switch-back]

Delete AP's second choice AC configuration.

no secondary-base

【Parameter Description】

Parameter	Description
ac-name	Configure the name of the AC. Up to 63 characters can be configured without spaces.
ip-address	The format is: A.B.C.D. AC's ip address.
switch-back	The switchback function is configured, and the switchback is not by default.

【Default Configuration】 N/A

【Command Mode】 AP configuration mode/all AP configuration mode

【Default Level】 15

【Usage Guide】 Configure the AP's redundant AC through the above command. primary-base is the preferred AC, secondary-base is the second option AC, tertiary-base is the third choice AC, backup-controller-primary is the fourth choice AC, backup-controller-secondary is the fifth choice AC, backup-controller-tertiary is the sixth choice AC.

The above command supports both ap-config ap-name and ap-config all configuration modes, according to the ap-config ap-name priority is higher than ap-config all to take effect.

【Configuration Example】 Set the second choice AC of AP ap1 to ac2, and the IP address of ac2 to 192.168.2.1

```
AC-FS#config terminal
AC-FS(config)#ap-config ap1
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.33 show ac-config

Display the basic configuration information of this AC。

show ac-config

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Arbitrary mode

【Default Level】 1

【Usage Guide】 N /A

【Configuration Example】 Basic configuration information of this AC.

```
AC-FS(config)#show ac-config
AC Configuration info:
Max_WTP: 128
STA_Limit: 4096
License Wtp max: 128
License STA Max: 4096
Serial Auth: Disable
Password Auth: Disable
Certificate Auth: Disable
Bind AP MAC: Disable
```

```
AP Priority: Disable
AC_Name: AC-FS_Ac_231455
AC Location: AC-FS_COM
AC State Info:
STA_Num: 0
Act_Wtp: 12
Used    Wtp: 8( 4 normal 8 half)
Remain    Wtp: 120 normal 240 half HW Ver 1.0
SW Ver: AC_RGOS 11.1(1)B1
Mac Address: 001a.9923.1455
Product ID: WS5708
NET ID: 9876543210012345
NAS ID: 001a.9923.1455
```

1.34 show ac-config ap-backup-group

Display the AP backup group information of this AC

show ac-config ap-backup-group [group-name]

【Parameter Description】

Parameter	Description
group-name	The name of the created AP backup group, optional, and the information of the default group is not displayed.

【Command Mode】 Arbitrary mode

【Default Level】 1

【Usage Guide】 N/A

【Configuration Example】 1: Display the AP backup group information of this AC.

```
AC-FS#show ac-config ap-backup-group
Cnt    Group-Name                Master-AP cnt Standby-AP cnt    Master-AP-Name      Working
_____  ________________________________________ _____________ _____________ _____________ _____________
1      AP-BACKUP-GROUP1          1             2                AP4210-1            false
```

2: Display detailed information of AP backup group AP-BACKUP-GROUP1.

```
AC-FS#show ac-config ap-backup-group AP-BACKUP-GROUP1

Cnt     Ap-Name                         Ap-Mac          Online    Is-Master Inherit-Wlan Cnt

1       AP4210-1                        8832.0000.1111  true      Yes       0
2       APD-M-1  false          No              0
```

【Prompt Information】 -

【Platform Description】 -

1.35 show ap-config bssid

Display the BSSID list of all AP.

show ap-config bssid

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Arbitrary mode

【Default Level】 1

【Usage Guide】 None

【Configuration Example】 1: View the BSSID list of all AP.

```
AC-FS(config)#show ap-config bssid

AP Mac          AP Name                                 Radio ID WLAN ID AP WLAN ID BSSID
```

【Prompt Information】 -

【Platform Description】 -

1.36 show ap-config bssid cb

Display the BSSID list of the specified AP and the mapping relationship between the AP WLAN ID corresponding to the AC WLAN ID.

show ap-config bssid cb ap-name

【Parameter Description】

Parameter	Description
ap-name	Specify the name of the AP.

【Command Mode】 Arbitrary mode

【Default Level】 1

【Usage Guide】 N/A

【Configuration Example】 1: View the BSSID list of the specified AP and the mapping relationship of the AP WLAN ID corresponding to the AC WLAN ID.

```
AC-FS#show ap-config bssid cb ap1
Radio ID WLAN ID AP WLAN ID BSSID
_________ _________ ___________ _______________
                                                1        101       1        06d0.f822.3355
1        102       2        0ad0.f822.3355

2        101       1        06d0.f822.3356
```

【Prompt Information】 -

1.37 show ap-config cb

Display AP status information.

show ap-config cb ap-name

【Parameter Description】 -

【Command Mode】 Privilege mode

【Default Level】 1

【Usage Guide】None

【Configuration Example】 1: Displays the status information of the AP.

```
ac#show ap-config cb wlan-ap-0001 Configuration:
ap name              :wlan-ap-0001 ap
fallback          :1
group name           :default
  Status:
local ipv4.....192.168.120.2
WTP Name             :wlan-ap-0001
```

【Prompt Information】 -

【Platform Description】 -

1.38 show ap-config inherit-wlan

Display the WLAN information inherited by the backup AP of the AP backup group.

show ap-config inherit-wlan ap-name

【Parameter Description】

Parameter	Description
ap-name	The name of the AP to be queried

【Command Mode】 Privileged mode

【Default Level】 1

【Usage Guide】 N/A

【Configuration Example】 1: Display the WLAN information inherited by the backup AP.

```
ac#show ap-config inherit-wlan wlan-ap-0001
WLAN ID SSID                    VLAN-Id/VLAN-Group ID    Radio ID                    AP WLAN ID
_______ ______________________ ______________________ ______________________ ___________

1       AC-FS-wifi              1100                     ALL                         1
```

【Prompt Information】 -

【Platform Description】 -

1.39 show ap-config product

Display AP product statistics list.

show ap-config product

【Parameter Description】 -

【Command Mode】 Privileged mode

【Default Level】 1

【Usage Guide】 N/A

【Configuration Example】 1: Display AP product statistics list.

```
AC-FS#show ap-config product
Product ID              Hardware Version Count   Used Wtp
_________________________________________________________

AP120                                1.0          10          5.0 AP220-E
1.0          5          5.0 AP320                                2.0
8          8.0 AP530-PPC                                1.5          2
```

【Prompt Information】 -

【Platform Description】 -

1.40 show ap-config summary

Show AP list.

show ap-config summary

【Parameter Description】 -

【Command Mode】 Privileged mode

【Default Level】 1

【Usage Guide】 None

【Configuration Example】 1: Show AP list.

```
AC-FS#show ap-config summary

========= show ap status =========

Radio:    Radio ID or Band:    2.4G = 1#, 5G = 2#

          E = enabled, D = disabled, N = Not exist

          Current Sta number

          Channel:    * = Global

          Power Level = Percent

Online AP number:    2 Offline AP number:    1

AP Name                    IP Address     Mac Address    Radio                  Radio Up/Off time    State
```

【Prompt Information】 -

【Platform Description】 -

1.41 show ap-config summary ap-auth

Display certification related information of all AP.

show ap-config summary ap-auth

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged Mode

【Default Level】 1

【Usage Guide】 -

【Configuration Example】 1: Display certification related information of all AP.

```
AC-FS#sh ap-config summary ap-auth
AP Name                          Mac     Address         Bind    bind-ap-serial      Bind    bind-ap-cert Bind
bind-ap-password Bind State
-------------------------------------------------------------------------------------------------------------------

ap220       1414.4b13.9ff3 FALSE                    TRUE
FALSE           TRUE Run
0011.0000.0101                  FALSE           TRUE                            FALSE           TRUE Quit
0011.0000.0201                  FALSE           TRUE
FALSE           TRUE    Quit
```

【Prompt Information】 -

【Platform Description】 -

1.42 show ap-config summary deny-ap

Display a list of AP that tried to associate but were rejected by the AC.

show ap-config summary deny-ap

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】 1

【Usage Guide】The capacity of the list entries is consistent with the capacity of the number of online AP supported by the AC.

【Configuration Example】 1: Display a list of AP that tried to associate but were rejected by the AC.

It contains AP name, AP IP address, AP MAC address, and reason for rejection information.

```
AC-FS#sh ap-config summary deny-ap
AP Name        IP Address          Mac Address      Reason
____________   ________________   ______________  - - ____________
 AP1                192.168.10.10    1414.4b13.9ff3  By  bind-ap-mac  AP2                192.168.10.11
00d0.f822.33b0    By bind-ap-mac
```

【Prompt Information】 -

【Platform Description】 -

1.43 show ap-group aps

Display the list of AP connected to the specified AP group.

show ap-group aps ap-group-name

【Parameter Description】

Parameter	Description
ap-group-name	AP group name

【Command Mode】 Privileged Mode

【Default Level】 1

【Usage Guide】 N/A

【Configuration Example】 1: Basic configuration information of this AC.

```
AC-FS(config)#show ap-group aps default
Ap Name                    Mac Addr          Pid
_____________________  _______________  _____________________-
rrm-ap                    0011.1122.3333 AP220E
```

【Prompt Information】 -

【Platform Description】 -

1.44 show ap-group aps summary

Display the AP list of all AP groups.

show ap-group aps summary

【Parameter Description】 -

【Command Mode】 Privileged mode

【Default Level】 1

【Usage Guide】 N/A

【Configuration Example】 1: View the AP list of all AP groups.

```
AC-FS(config)#show ap-group aps summary

Ap Name                                    AP                                    group ctx_name
AC DESCRIPTION
-----------------------------------------------------------------------------------------------

ap100                    default          192.168.201.199-1          AC199
```

【Prompt Information】 -

【Platform Description】 -

1.45 show ap-group cb

Display the basic configuration information of the specified AP group.

show ap-group cb ap-group-name

【Parameter Description】

Parameter	Description
ap-group-name	AP group name

【Command Mode】 Privileged mode

【Default Level】 1

【Usage Guide】 N/A

【Configuration Example】 1: Display the basic configuration information of the default AP group.

```
AC-FS(config)#show ap-group cb default
Ap Group info:
apg_name        : default ap_fallback     : Enable hb_ctx_id              : 2
```

【Prompt Information】 -

【Platform Description】 -

1.46 show ap-group intf-wlan-map

Display the WLAN-VLAN mapping of the specified AP group.

show ap-group intf-wlan-map ap-group-name

【Parameter Description】

Parameter	Description
ap-group-name	AP group name

【Command Mode】 Privileged mode

【Default Level】 1

【Usage Guide】 N/A

【Configuration Example】 1: Display the WLAN-VLAN mapping of the AP group

```
AC-FS#show ap-group intf-wlan-map apg-1

WLAN ID  SSID                          VLAN-Id/VLAN-Group ID  Radio                ID AP
WLAN ID  Enable

-------------------------------------------------------------------------------------------

1        test-web-11                   110                    ALL
1                True
2        test-802.1x-11                111                    ALL
2                True
3        test-iphone-11                112                    ALL
3                True
4        test-guest-11                 113                    ALL
4                True
```

【Prompt Information】 -

【Platform Description】 -

1.47 show ap-group summary

Display the list of all AP groups configured by this AC.

show ap-group summary

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】 1

【Usage Guide】 None

【Configuration Example】 1: Display the list of all AP groups configured by this AC

```
AC-FS(config)#show ap-group summary Total Ap Group Num :  2
Ap Group Name
1.  default 2. test-group
```

【Prompt Information】 -

【Platform Description】 -

1.48 show ap-mode

Show AP fat or fit mode.

show ap-mode

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】 1

【Usage Guide】None

【Configuration Example】 1: Display AP's fat and fit mode.

```
AC-FS#show ap-mode
current mode:  FIT
```

【Prompt Information】 -

【Platform Description】 -

1.49 show license

This command is used to view the status of AP support after the license is installed on the AC.

show license

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】 1

【Usage Guide】 N/A

【Configuration Example】 1: Display the license installation status on the AC.

```
AC-FS#show license

Serial Number    :   xxxxxxxxxxxxx

 No. Activation Key                                  AP Number
-----------------------------------------------------------------------------------------

   1. AAAA-BBBB-CCCC-DDDD-EEEE-FFFF-GGGG-HHHH        128
-----------------------------------------------------------------------------------------

Total 272 access points are supported, old version 128, new version 16. AC-FS#
```

【Prompt Information】 There are two versions of License, one is that the string form is regarded as the old version of the license, the other is that the file format is regarded as a new version of the license; Activation Key shows the details of the old version of the license, the detailed information of the new version of the license is displayed in show license all-license.

【Platform Description】 -

1.50 show ap-group radios

Display the AP radio statistics of all AP groups in this AC.

show ap-group radios

【Parameter Description】 -

【Command Mode】 Privileged mode

【Default Level】 1

【Usage Guide】 None

【Configuration Example】 1: Display the AP radio statistics of all AP groups in this AC.

```
AC-FS#show ap-group radios
 Total Ap Group Num :  2
Total Aps radio Sum :  50
Note:  The online radio number of AP is calculated according to the capacity value of AP. Eg:  ap130(L) is calculated as 2,
```

【Prompt Information】 -

【Platform Description】 Only AC supported

1.51 show wlan hot-backup

This command is used to view the instance list of the backup peer.

show wlan hot-backup [peer-ip] summary

【Parameter Description】

Parameter	Description
peer-ip	Specify the IP address of the backup peer.

【Command Mode】 Privileged mode

【Default Level】 1

【Usage Guide】 Use this command on the central AC to view the number of licenses allocated by the central AC to the branch AC

and the number of licenses of the backup branch AC.

【Configuration Example】 1: View the instance list of all backup peers.

```
AC-FS#show wlan hot-backup summary

Context Name                    AC DESCRIPTION                    AP Num STA Num
_____________________________ _____________________________ _________ _________

192.168.201.76-11               AC-76                             1         0
192.168.201.77-1        AC-77                 2     1
```

2: View the instance list of the specified backup peer.

```
AC-FS#show  wlan  hot-backup  192.168.201.76  summary  Context  AC

DESCRIPTION                    AP Num STA Num
_________  ____________________________________  _________  _________

11        AC-76                 1         2
```

3: Central AC View the list of instances of all backup peers.

```
AC-FS#show wlan hot-backup summary
Context Name        AC DESCRIPTION          AP Num STA Num Assigned Lic Backups Lic
-------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------

192.168.201.76-11          AC-76                 1     0         32
64
192.168.201.77-1          AC-77                 2     1         16
32
192.168.201.78-1          AC-78                 11    30        NA                NA
192.168.201.81-100        AC-100                5     24    NA                NA
```

4: The central AC view the instance list of the specified backup peer.

```
AC-FS#show wlan hot-backup 192.168.201.76 summary

Context AC DESCRIPTION                    AP Num STA Num Assigned Lic Backups Lic
                                 11        AC-76                        1        2        32        64
```

【Prompt Information】 -

【Platform Description】 -

1.52 show wlan-config cb

This command is used to view the WLAN details on the AC.

show wlan-config cb

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】 1

【Usage Guide】 None

【Configuration Example】 1: View the WLAN configuration list on the AC.

```
AC-FS(config)#show wlan-config cb      512 WLAN ID  512
SSID  ssid-512
Profile        <NULL>
Short Preamble    Disable
Spectrum ManagementDisable
QoS   Disable
Short Slot Time    Disable
APSD Disable
Delayed Block ACK       Disable
Immediate Block ACK    Disable
MAC Mode Local
```

【Prompt Information】 -

1.53 show wlan-config summary

This command is used to view the WLAN configuration list on the AC.

show wlan-config summary

【Parameter Description】 -

【Command Mode】 Privileged mode

【Default Level】 1

【Usage Guide】 N/A

【Configuration Example】 1: View the WLAN configuration list on the A

```
AC-FS(config)#show wlan-config summary Total Wlan Num :    3
Wlan id Profile Name              SSID              STA NUM
                          1              pro-1                        ssid-1                0
_________  ____________________________  ____________________________  _________
2           pro-2                        ssid-2           0
4095       <NULL>                        ssid-4095                0
```

【Prompt Information】 -

【Platform Description】 -

1.54 ssid

Modify the SSID name through ssid in WLAN configuration mode.

ssid ssid-string

【Parameter Description】

Parameter	Description
ssid-string	ssid string with a maximum length of 32 characters.

【Default Configuration】 -

【Command Mode】 WLAN configuration mode

【Default Level】 15

【Usage Guide】 If the WLAN has been deployed, this command will cause the user currently associated with the WLAN to go offline.

【Configuration Example】 1: Modify the SSID name of the WLAN with ID 1 to AC-FS.

```
AC-FS(config)#wlan-config 1
```

【Verification】 Use show wlan-config summary to view all wlan information.

```
AC-FS(config)#show    wlan-config    summary    Total
Wlan Num :    2
Wlan id Profile Name              SSID              STA NUM
_________  ________________________  ________________________  _________
1              pro-1                        AC-FS                      0
2             pro-2                       ssid-2            0
```

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.55 ssid-code

Modify the character set of SSID in WLAN by configuring the character set of SSID in WLAN.

ssid-code {gbk | utf-8}

【Parameter Description】

Parameter	Description
gbk	Use gbk coded character set.
utf-8	Use utf-8 coded character set.

【Default Configuration】 None, follow the uniform coded character set of the device.

【Command Mode】 WLAN configuration mode

【Default Level】 15

【Usage Guide】1: If the WLAN has been deployed, this command will cause the user currently associated with the WLAN to go offline.

2: Part of wireless stations may only support utf-8/gbk coded character set, and when the ssid name is Chinese, this part of the terminal cannot be associated. In this case, you can modify the ssid name to utf-8/gbk through ssid-code to adapt to the wireless stations.

【Configuration Example】 1: Modify the SSID name of the WLAN with ID 1 to use utf-8 coded character set.

```
AC-FS(config)#wlan-config 1

AC-FS(config-wlan)#ssid-code utf-8
```

【Verification】 View the ssid-code of the WLAN configuration through the show running-config command.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 Only AC supported

1.56 statistics-timer

In the configuration mode, use statistics-timer to set the time interval for the specified AP or all APs in the specified AP group to upload statistical information regularly.

statistics-timer timer-num

Restore to the default value.

no statistics-timer

【Parameter Description】

Parameter	Description
timer-num	The timer interval to be set, in seconds, value range: 1~65535.

【Default Configuration】 By default, the timer is 120s.

【Command Mode】 AP configuration mode or AP group configuration mode

【Default Level】 15

【Usage Guide】 Set the statistics timer of the specified AP. This command can restore the default value of statistics timer through the no prefix.

【Configuration Example】 1: Enter AP0001 configuration mode, and configure its statistics timer to 200s.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# statistics-timer 200
```

2: Enter AP0001 configuration mode, and configure its statistics timer to restore the default value of 120s.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# no statistics-timer
```

3: Enter the default AP group and configure its statistics timer to 200s.

```
AC-FS(config)# ap-group default
AC-FS(config-ap-group)# statistics-timer 200
```

4: Enter the default AP group, and configure its statistics timer to restore the default value of 120s.

```
AC-FS(config)# ap-group default
AC-FS(config-ap-group)# no statistics-timer
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.57 switch2-fat

Use the switch2fat command to configure the specified AP to switch to fat AP mode. This command will cause the specified AP to leave the AC.

switch2fat ap-name

【Parameter Description】

Parameter	Description
ap-name	The name of the AP

【Default Configuration】 By default, all thin APs are controlled by the associated AC, and thin APs can be converted into fat APs, which means they can have self-control ability.

【Command Mode】AC configuration mode

【Default Level】 15

【Usage Guide】 Configure the specified AP to switch to the fat AP mode. This command will cause the specified AP to leave the AC. In fit mode, the default login password for user mode is AC-FS, and the default login password for privileged mode is apdebug.
In fat mode, the default login password for user mode is admin, and there is no default login password for privileged mode.

【Configuration Example】1: Configure AP0002 to switch to fat mode.

```
AC-FS(config-ac)#switch2fatAP0002
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.58 tertiary-base

Configure AP's third choice AC.

tertiary-base ac-name { ip-address } [switch-back]

Delete the third choice AC configuration of the AP.

no tertiary-base

【Parameter Description】

Parameter	Description
ac-name	Delete the third choice AC configuration of the AP
ip-address	The format is: A.B.C.D. The ip address of the AC.
switch-back	The switchback function is configured, and the switchback is not by default.

【Default Configuration】 N/A

【Command Mode】 AP configuration mode/all AP configuration mode

【Default Level】 15

【Usage Guide】 Configure the AP's redundant AC through the above command. primary-base is the preferred AC, secondary-base is the second option AC, tertiary-base is the third choice AC, backup-controller-primary is the fourth choice AC, backup-controller-secondary is the fifth choice AC, backup-controller-tertiary is the sixth choice AC.

The above command supports both ap-config ap-name and ap-config all configuration modes, according to ap-config, ap-name takes effect higher than ap-config all.

【Configuration Example】 Set the third choice AC of AP ap1 to ac3, and the IP address of ac3 to 192.168.3.1.

```
AC-FS#config terminal
AC-FS(config)#ap-config ap1
```

```
AC-FS(config-ap)#tertiary-base ac3
192.168.3.1
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.59 wlan-config

In the configuration mode, create a WLAN through wlan-config and enter the WLAN configuration mode.

wlan-config wlan-id [profile-string] [ssid-string]

Delete WLAN.

no wlan-config wlan-id

【Parameter Description】

Parameter	Description
wlan-id	The ID of the WLAN to be created, the value range is 1~4094.
profile-string	Descriptor of the WLAN, can be omitted, the maximum length is 32 characters.
ssid-string	The ssid string corresponding to the WLAN, the maximum length is 32 characters.

【Default Configuration】 N/A

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】 Create a WLAN, such as the command description, must specify ssid-string, profile-string can be omitted; After creating a WLAN, CLI will automatically enter the configuration mode of the WLAN;

Enter the configuration mode of a WLAN, you only need to specify the existing WLAN ID. You can enter the configuration mode corresponding to the WLAN.

One SSID can correspond to multiple WLAN, but one WLAN cannot be associated with multiple SSID at the same time.

【Configuration Example】 1: Create a WLAN with ID 2048, and the ssid of the WLAN is ssid-test.

```
AC-FS(config)#  wlan-config  2048  profile-test  ssid-test
AC-FS(config-wlan)# exit
```

2: Enter the created WLAN configuration mode with ID 2048.

```
AC-FS(config)#  wlan-config  2048
AC-FS(config-wlan)# exit
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.60 wtp-limit

Configure the maximum number of AP supported on the AP through wtp-limit.

wtp-limit wtp-num

Restore Defaults.

no wtp-limit

【Parameter Description】

Parameter	Description
wtp-num	The maximum number of AP that AC can connect to.

【Default Configuration】 By default, this value is equal to the number of APs supported by each AC model.

【Command Mode】 AC configuration mode

【Default Level】 15

【Usage Guide】 Configure the maximum number of AP supported on the AC. The number cannot exceed the maximum value supported by the AC, nor can it exceed the maximum value allowed by the license.

Different types of AP occupy different weights (For example, WALL-AP, two APs occupy one AP number), AC will calculate the actual number of weighted AP based on the weight coefficient when accessing the AP. This command and license control the number of weighted APs instead of the actual number of AP.

【Configuration Example】 1: The user configures the AC to connect up to 100 AP.

```
AC-FS(config-ac)# wtp-limit 100
```

2: The user configures the maximum number of AP that can be connected to the AC as the default value.

```
AC-FS(config-ac)# no wtp-limit
```

【Verification】 View the maximum number of APs that can be connected to the configured AC through the show ac-config command.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

2 STAMG

2.1 ap

Configure AP information in the domain in the associated control domain configuration mode.

ap WORD

The user can use the no option of this command to delete the specified AP from the associated control domain.

no ap [WORD]

【Parameter Description】

Parameter	Description
WORD	AP name. Length [1-64].

【Default Configuration】 There is no AP information in the associated control domain.

【Command Mode】 Associated control domain configuration mode.

【Default Level】 15

【Usage Guide】 Up to 5 AP information can be configured in one associated control domain, if it exceeds, the system will give a corresponding error prompt. In addition, when configuring AP information for the associated control domain, the AP is not required to be online.

【Configuration Example】 1: Configure an AP with a MAC address of 00d0.f800.1001 for the associated control domain named "first class".

```
AC-FS(config)#control-zone first class
AC-FS(config- cznoe)# ap 00d0.f800.1001
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.2 assoc-control

Enable association control function.

assoc-control

The user can use the no option of this command to turn off the associated control function.

no assoc-control

【Parameter Description】 -

【Default Configuration】 The default association control function is turned off

【Command Mode】 Global configuration mode

【Default Level】15

【Usage Guide】 When the related control function is not enabled, the related commands of the related control are still configurable, but the function does not work.

【Configuration Example】 1: Turn on the link control function:

```
AC-FS(config)#assoc-control
```

2: Turn off the link control function:

```
AC-FS (config)#no assoc-control
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.3 lient-kick

Configure and delete the MAC address of the specified wireless user through the client-kick command.

client-kick sta-mac

【Parameter Description】

Parameter	Description
sta-mac	MAC address of wireless user.

【Default Configuration】 N/A

【Command Mode】 AC configuration mode

【Default Level】 15

【Usage Guide】 None

【Configuration Example】 1: Delete the wireless user whose MAC address is aaaa.bbbb.cccc.

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# client-kick aaaaa.bbbbb.ccccc
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

【Usage Guide】 N/A

【Configuration Example】 1: Delete the wireless user whose MAC address is aaaa.bbbb.cccc.

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# client-kick aaaaa.bbbbb.ccccc
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.4 control-zone

Create an associated control domain and enter the associated control domain configuration mode.

control-zone czone-name

The user can use the no option of this command to delete the specified associated control domain configuration.

no control-zone czone-name

【Parameter Description】

Parameter	Description
czone-name	Associated control domain name, length [1,64].

【Default Configuration】 No associated control domain configuration.

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】 Up to 300 associated control domains can be configured on the AC, if the limit is exceeded, an error message will be issued.

【Configuration Example】 1: Configure an associated control domain named "class 1".

```
AC-FS(config)#control-zone class 1
AC-FS(config- czone)#
```

2: Delete the associated control domain named "class 1".

```
Continue? [no] y
AC-FS(config)#
```

```
AC-FS(config)# no control-zone class 1
The opreration will clear the control zone configuration, which may cause corresponding STAs
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.5 flow-balance-group add

Use the flow-balance-group add command to configure to add the specified AP to the specified load balancing group.

flow-balance-group add group-name ap-name

【Parameter Description】

Parameter	Description
group-name	Specify the name of the balance group, each traffic balance group supports a maximum of 10 AP.
ap-name	Name of AP to be added.

【Default Configuration】 No AP in the load balancing group.

【Command Mode】 AC configuration mode

【Default Level】 15

【Usage Guide】 N/A

【Configuration Example】 1: Add the two AP named ap1 and ap2 to the balance group test-group.

```
AC-FS(config)# ac-controller
AC-FS(config-ac)#  flow-balance-group  add  test-group  ap1
AC-FS(config-ac)# flow-balance-group add test-group ap2
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.6 flow-balance-group base

Use the flow-balance-group base command to configure the flow base value used for flow load balancing.

flow-balance-group base number

The restoration reference value is Default Configuration (10Mbps).

no flow-balance-group base

【Parameter Description】

Parameter	Description
number	The traffic reference value, the default is 10Mbps, and the range is 1-100.

【Default Configuration】 The benchmark value is 10Mbps.

【Command Mode】 AC configuration mode

【Default Level】 15

【Usage Guide】 N/A

【Configuration Example】 1: Configure the traffic base value for traffic load balancing to be 50Mbps.

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# flow-balance-group base 50
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.7 flow-balance-group create

Use the flow-balance-group create command to configure and create a flow-based load balancing group.

flow-balance-group create group-name

Delete the traffic-based load balancing group.

no flow-balance-group create group-name

【Parameter Description】

Parameter	Description
group-name	The name of the load balancing group can be configured with up to 55 characters and cannot contain spaces. Support up to creation 80 traffic balancing groups.

【Default Configuration】 No load balancing group created.

【Command Mode】 AC configuration mode

【Default Level】 15

【Usage Guide】No operation is used to delete the specified balance group configuration.

【Configuration Example】 1: Create a load balancing group named test-group.

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# flow-balance-group create test-group
```

2: Delete the load balancing group named test-group.

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# no flow-balance-group create test-group
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.8 flow-balance-group del

Use the flow-balance-group del command to configure to delete the specified AP from the specified load balancing group.

flow-balance-group del group-name ap-name

【Parameter Description】

Parameter	Description
group-name	The load balancing group to be operated.
ap-name	The name of the AP to be removed from the balance group.

【Default Configuration】 N/A

【Command Mode】 Global configuration mode

【Default Level】 15

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.9 flow-balance-group enable

Configure the start threshold of the balance group through the flow-balance-group enable command. Only when the traffic of the currently associated AP reaches the threshold, the traffic load balancing function is activated.

flow-balance-group enable group-name number

The load threshold of the restoration balance group is Default Configuration.

no flow-balance-group enable group-name number

【Parameter Description】

Parameter	Description
group-name	The name of the load balancing group to be operated.
number	The start threshold of the balance group, the unit is %, the default is 5%, the range is 0-500, where 0 means that the balance group does not enable the flow balance function. The default percentage is 10Mbps.

【Default Configuration】 Starting threshold 5%.

【Command Mode】 AC configuration mode

【Default Level】 15

【Usage Guide】 N/A

【Configuration Example】 1: Configure the threshold of the balance group named test-group to 100kbps.

```
AC-FS(config)# ac-controller

AC-FS(config-ac)# flow-balance-group enable test-group 1
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.10 flow-balance-group flow

Use the flow-balance-group flow command to configure the load threshold of the balance group.

flow-balance-group flow group-name number

The load threshold of the restoration balance group is Default Configuration.

no flow-balance-group flow group-name number

【Parameter Description】

Parameter	Description
group-name	The name of the load balancing group to be operated.
number	The start threshold of the balance group, the unit is %, the default is 5%, the range is 0-500, where 0 means that the balance group does not enable the flow balance function. The default percentage is 10Mbps.

【Default Configuration】 Flow threshold 5%.

【Command Mode】 AC configuration mode

【Default Level】 15

【Usage Guide】 N/A

【Configuration Example】 1: Configure the threshold of the balance group named test-group to be 100kbps.

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# flow-balance-group flow test-group 1
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# flow-balance-group flow test-group 1
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.11 flow-balance-group radio-flow

The flow-balance-group radio-flow command is used to configure the balance group to support load balancing under local forwarding. The balance group will use the traffic regularly uploaded by the AP instead of the real-time statistics on the AC for balance judgment.

flow-balance-group radio-flow group-name

Resume to use AC real-time statistics for load balancing judgment.

no flow-balance-group radio-flow group-name

【Parameter Description】

Parameter	Description
group-name	The name of the load balancing group to be operated.

【Default Configuration】 Traffic counted by CAPWAP data channel on AC.

【Command Mode】 AC configuration mode

【Default Level】 15

【Usage Guide】None

【Configuration Example】 1: Configure the balance group named test-group to switch to using the traffic sent from the AP at regular intervals.

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# flow-balance-group radio-flow test-group
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.12 hide-SSID STA-reach-limit

Configure the smart hide SSID function through the hide-ssid sta-reach-limit command, When the AP reaches the maximum number of users, the ssid on the radio with this function turned on on the AP will be hidden, when the number of users on a single radio reaches the upper limit, the ssid on the radio will be hidden to prevent the new STA from trying to associate and failing to associate.
Restore the default configuration.

no hide-ssid sta-reach-limit [radio { 2.4g | 5g }]

【Parameter Description】

Parameter	Description
Radio	Specify the command to enable this function on a specific radio, and enable it on all radios if not specified.
2.4G	Enable this function on 2.4g radio.

5G	Enable this function on 5g radio.

【Default Configuration】 Hide SSID function is not enabled.

【Command Mode】 AC is AP configuration mode, fat AP is global configuration mode.

【Default Level】 15

【Usage Guide】 After the Smart Hide SSID function is enabled, if the APs in an area reach the user limit, new users cannot scan the SSID in this area.

【Configuration Example】 1: AP-config all configuration, enable the smart hidden SSID function of 5g radios of all AP.

```
AC-FS(config)# ap-config all

AC-FS(config-ap)# hide-ssid sta-reach-limit radio 5g
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 Need to be supported by AC/AP for the function to take effect. If it is supported on the AC, the command can be configured, but if the AP version does not support it, the function will not take effect.

【Platform Description】 AC, fat AP

2.13 inter-radio-balance flow-balance dual-band

Configure different frequencies for AP or AP group (2.4G and 5G) Inter-radio traffic load balancing start threshold and threshol.

inter-radio-balance flow-balance dual-band enable-load en-num threshold thrs-num.

Restore the traffic load balancing parameters among radios of different frequencies in the AP or AP group to the default values.

no inter-radio-balance flow-balance dual-band.

【Parameter Description】

Parameter	Description

en-num	Start thres starhold, that is, the current traffic on the associated radio exceeds this value tot load balancing. The unit is 100Kbps, and the range of values is 1-1000.
thrs-num	Balance threshold, when the difference between the traffic on the currently associated radio and the radio with the lowest load exceeds this value, Reject STA to associate with this radio. The unit is 100Kbps, and the value range is 1-1000.

【Default Configuration】 By default, the startup threshold is 10 (1Mbps),The equalization threshold is 10 (1Mbps).

【Command Mode】 AP configuration mode or AP group configuration mode.

【Default Level】 15

【Usage Guide】 If the traffic load balance between the radios of the specified AP is enabled, The load of the radio that the STA intends to associate with exceeds the start threshold, and the difference from the minimum load exceeds the threshold, STA will be refused association, to guide to the radio with lower load. This configuration only takes effect when the radio with the lowest load.
and the radio associated with the intention are of different frequencies, if the frequency is the same, the configuration of inter-radio-balance flow-balance same-band takes effect.

【Configuration Example】 1: Configure AP0001 to start the threshold and threshold of traffic load balancing between radios of different frequencies to 800Kbps.

```
AC-FS(config)# ap-config AP0001
```

2: Restore AP0001's inter-radio traffic load balancing configuration of different frequencies to the default value.

```
AC-FS(config)# ap-config AP0001
```

3: Configure the default AP group's inter-radio traffic load balancing threshold for different frequencies to be 300Kbps, and the threshold is 500Kbps.

```
AC-FS(config)# ap-group default
AC-FS(config-group)# inter-radio-balance flow-balance dual-band enable-load 3 threshold 5
```

4: Configure the start threshold and threshold of traffic load balancing between radios of different frequencies of all APs to 3Mbps.

```
AC-FS(config)# ap-config all
AC-FS(config-ap)# inter-radio-balance flow-balance dual-band enable-load 30 threshold 30
```

【Verification】 -

【Prompt Information】

【Common Mistake】 -

【Platform Description】 AC

2.14 inter-radio-balance flow-balance enable

Enable inter-radio traffic load balancing of AP or AP group.

inter-radio-balance flow-balance enable

Disable the load balancing of traffic between radios of AP or AP group.

no inter-radio-balance flow-balance enable

【Parameter Description】 -

【Default Configuration】 By default, traffic load balancing between radios is disabled.

【Command Mode】 AP configuration mode or AP group configuration mode

【Default Level】15

【Usage Guide】After enabe load balancing of traffic between radios of a specified AP, AC will try to ensure that the difference in user traffic between radios of this AP does not exceed the threshold.

【Configuration Example】 1: Enable AP0001 inter-radio traffic load balancing.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# inter-radio-balance flow-balance enable
```

2: Disable AP0001 inter-radio traffic load balancing.

```
AC-FS(config)# ap-config AP0001
```

3: Enable load balancing of inter-radio traffic of APs in the default AP group.

```
AC-FS(config)# ap-group default
```

4: Enable all AP's inter-radio traffic load balancing.

```
AC-FS(config)# ap-config all
AC-FS(config-ap)# inter-radio-balance flow-balance enable
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.15 Inter-Radio-Balance Flow-Balance Same-Band

Configure the start threshold and threshold value of traffic load balancing between the same frequency (2.4G or 5g) radios of AP or AP group.

inter-radio-balance flow-balance same-band enable-load en-num threshold thrs-num

Restore the traffic load balancing parameters between the same frequency radios in the AP or AP group to the default value.

no inter-radio-balance flow-balance same-band

【Parameter Description】

Parameter	Description
en-num	Start threshold, that is, the current traffic on the associated radio exceeds this value to start load balancing. The unit is 100kbps, and the value range is 1-1000.
thrs-num	Balance threshold, that is, when the difference between the traffic on the currently associated radio and

	the radio with the lowest load exceeds this value, reject STA to associate with this radio. The unit is 100kbps, and the value range is 1-1000.

【Default Configuration】 By default, the startup threshold is 5 (500Kbps), the equalization threshold is 5 (500Kbps).

【Command Mode】 AP configuration mode or AP group configuration mode

【Default Level】 15

【Usage Guide】 If the traffic load balancing between radios of the specified AP is enabled, the load of the radio that the STA intends to associate with exceeds the start threshold, and the difference with the minimum load exceeds the threshold, the STA will be refused association to guide to the radio with lower load. This configuration only takes effect when the lowest-load radio and the intent-associated radio have the same frequency, If the frequency is different, the configuration of inter-radio-balance flow-balance dual-band takes effect.

【Configuration Example】 1: Configure AP0001's inter-radio traffic load balancing start threshold and threshold to 800kbps.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# inter-radio-balance flow-balance same-band enable-load 10 threshold 10
```

2: Restore AP0001's inter-radio traffic load balancing configuration of the same frequency to the default value.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# no inter-radio-balance flow-balance same-band
```

3: Configure the default AP group's inter-radio traffic load balancing threshold for the same frequency to be 300kbps, and the threshold is 500kbps.

```
AC-FS(config)# ap-group default
AC-FS(config-group)# inter-radio-balance flow-balance same-band enable-load 3 threshold 5
```

【Platform Description】 AC

2.16 inter-radio-balance flow-balance same-band

Configure the start threshold and threshold value of traffic load balancing between the same frequency (2.4G or 5g) radios of AP or AP group.

inter-radio-balance flow-balance same-band enable-load en-num threshold thrs-num

Restore the traffic load balancing parameters between the same frequency radios in the AP or AP group to the default value.

no inter-radio-balance flow-balance same-band

【Parameter Description】

Parameter	Description
en-num	Start threshold, that is, the current traffic on the associated radio exceeds this value to start load balancing. The unit is 100kbps, and the value range is 1-1000.
thrs-num	Balance threshold, that is, when the difference between the traffic on the currently associated radio and the radio with the lowest load exceeds this value, reject STA to associate with this radio. The unit is 100kbps, and the value range is 1-1000.

【Default Configuration】 By default, the startup threshold is 5 (500Kbps), the equalization threshold is 5 (500Kbps).

【Command Mode】 AP configuration mode or AP group configuration mode

【Default Level】15

【Usage Guide】 If the traffic load balancing between radios of the specified AP is enabled, the load of the radio that the STA intends to associate with exceeds the start threshold, and the difference with the minimum load exceeds the threshold, the STA will be refused association to guide to the radio with lower load. This configuration only takes effect when the lowest-load radio and the intent-associated radio have the same frequency, If the frequency is different, the configuration of inter-radio-balance flow-balance dual-band takes effect.

【Configuration Example】 1: Configure AP0001's inter-radio traffic load balancing start threshold and threshold to 800kbps.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# inter-radio-balance flow-balance same-band enable-load 10 threshold 10
```

2: Restore AP0001's inter-radio traffic load balancing configuration of the same frequency to the default value.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# no inter-radio-balance flow-balance same-band
```

3: Configure the default AP group's inter-radio traffic load balancing threshold for the same frequency to be 300kbps, and the threshold is 500kbps.

```
AC-FS(config)# ap-group default
AC-FS(config-group)# inter-radio-balance num-balance enable
```

4: Restore AP0001's inter-radio quantity load balancing configuration of different frequencies to the default value.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# no inter-radio-balance num-balance dual-band
```

5: Configure the default load balancing threshold for the number of APs in the AP group between radios of different frequencies to 4, and the threshold to 5.

```
AC-FS(config)# ap-group default
AC-FS(config-group)# inter-radio-balance num-balance dual-band enable-load 4 threshold 5
```

6: Configure the number of load balancing start thresholds and thresholds for all APs between radios of different frequencies to 5.

```
AC-FS(config)# ap-config all
AC-FS(config-ap)# inter-radio-balance num-balance dual-band enable-load 5 threshold 5
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.17 inter-radio-balance num-balance enable

Enable load balancing of the number of radios in AP or AP group.

inter-radio-balance num-balance enable

Disable AP or AP group inter-radio quantity load balancing.

no inter-radio-balance num-balance enable

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 By default, the number load balancing between radios is disabled.

【Command Mode】 AP configuration mode or AP group configuration mode.

【Default Level】 15

【Usage Guide】 After enable the load balancing of the number of radios of a specified AP, the AC will try to ensure that the difference in the number of users between the radios of the AP does not exceed the threshold.

【Configuration Example】 1: Enable AP0001 inter-radio quantity load balance.

```
AC-FS(config)# ap-config AP0001

AC-FS(config-ap)# inter-radio-balance num-balance enable
```

2: Disable AP0001 inter-radio quantity load balance.

```
AC-FS(config)# ap-config AP0001

AC-FS(config-ap)# no inter-radio-balance num-balance enable
```

3: Enable load balance of the number of radios of AP in the default AP group.

```
AC-FS(config)# ap-group default

AC-FS(config-group)# inter-radio-balance num-balance enable
```

4: Enable load balancing of the number of radios of all AP.

```
AC-FS(config)# ap-config all

AC-FS(config-ap)# inter-radio-balance num-balance enable
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.18 inter-radio-balance num-balance same-band

Configure AP or AP group's same frequency (the same 2.4G or 5G) radio quantity load balancing start threshold and threshold.

inter-radio-balance num-balance same-band enable-load en-num threshold thrs-num

Restore the load balancing parameters of the number of radios on the same frequency in the AP or AP group to the default value.

no inter-radio-balance num-balance same-band

【Parameter Description】

Parameter	Description
en-num	Start threshold, that is, the number of currently associated radios exceeds this value to start load balancing. Value range is 1-20 users.
thrs-num	Balance threshold, that is, when the difference between the number of currently associated radios and the number of radios with the lowest load exceeds this value,Reject STA to associate with this radio. Value range is 1-20.

【Default Configuration】 By default, the start threshold is 2 and the equalization threshold is 2.

【Command Mode】 AP configuration mode or AP group configuration mode.

【Default Level】 15

【Usage Guide】 If the number of radios of the specified AP is load balancing enabled, The load of the radio that the STA intends to associate with exceeds the start threshold, and the difference from the minimum load exceeds the threshold, the STA will be refused association to guide to the radio with lower load. This configuration only takes effect when the lowest-load radio and the intent-associated radio have the same frequency, If the frequency is different, the configuration of inter-radio-balance num-balance dual-band takes effect.

【Configuration Example】 1: Configure AP0001's number of same-frequency radios to load balancing start threshold and threshold to 3.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# inter-radio-balance num-balance same-band enable-load 3 threshold 3
```

2: Restore AP0001's inter-radio number load balancing configuration of the same frequency to the default value.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# no inter-radio-balance num-balance same-band
```

3: Configure the default load balancing threshold for the number of APs within the same frequency radio in the AP group to 3, and the threshold to 5.

```
AC-FS(config)# ap-group default
AC-FS(config-group)# inter-radio-balance num-balance same-band enable-load 3 threshold 5
```

4: Configure the load balancing start threshold and threshold of the number of radios on the same frequency of all APs to 5.

```
AC-FS(config)# ap-config all
AC-FS(config-ap)# inter-radio-balance num-balance same-band enable-load 5 threshold 5
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.19 inter-radio-balance radio weight

Configure the load ratio between radios during load balancing between radios, configure the weights of the radios, and the weight ratio is the load ratio.

inter-radio-balance radio radio-id weight weight-num

Restore the load weight of the radio to the default value.

no inter-radio-balance radio radio-id weight

【Parameter Description】

Parameter	Description
Radio-id	Specify a radio for weight configuration.
Weight-num	Weight value, value range 1-100, default 100.

【Default Configuration】 By default, the weight is 100, when load balancing between radios, balance according to the ratio 100: 100, 1: 1 balance.

【Command Mode】 AC is the AP configuration mode or AP group configuration mode, and the fat AP is the global configuration mode.

【Default Level】 15

【Usage Guide】 If you want radio 1 and radio 2 to be load balanced in a 1: 2 ratio, the weight of radio 1 can be configured as 50, then the load ratio of radio 1 to radio 2 is 50: 100 (1: 2).

【Configuration Example】 1: Configure the weight of radio 1 to 50, and load balance between radio 1 and radio 2 in a ratio of 1: 2.

```
AC-FS(config)# ap-config AP0001

AC-FS(config-ap)# inter-radio-balance radio 1 weight 50
```

2: Restore the weight of radio 1 to the default value, and load balance between radio 1 and radio 2 at a ratio of 1: 1.

```
AC-FS(config)# ap-config AP0001

AC-FS(config-ap)# no inter-radio-balance radio 1 weight
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC or fat AP

2.20 num-balance-group add

Use the num-balance-group add command to configure to add the specified AP to the specified load balancing group.

num-balance-group add group-name ap-name

【Parameter Description】

Parameter	Description
group-name	Specify the name of the balance group, each balance group supports up to 10 AP.
ap-name	The name of the AP to be added。

【Default Configuration】 No AP in the load balancing group.

【Command Mode】 AC configuration mode

【Default Level】 15

【Usage Guide】 N/A

【Configuration Example】 1: Add the AP named ap1 to the balance group test-group.

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# num-balance-group add test-group ap1
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.21 num-balance-group create

Use the num-balance-group create command to configure and create a quantity-based load balancing group.

num-balance-group create group-name

Delete the quantity-based load balancing group.

no num-balance-group create group-name

【Parameter Description】

Parameter	Description
Group-name	The name of the load balancing group, up to 55 characters can be configured, cannot contain spaces. Support up to creation 80 quantity balance groups.

【Default Configuration】 No load balance group created

【Command Mode】 AC configuration mode

【Default Level】 15

【Usage Guide】 N/A

【Configuration Example】 1: Create a load balancing group named test-group.

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# num-balance-group create test-group
```

2: Delete the load balancing group named test-group.

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# no num-balance-group create test-group
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.22 num-balance-group del

Use the num-balance-group del command to configure to delete the specified AP from the specified load balancing group.

num-balance-group del group-name ap-name

【Parameter Description】

Parameter	Description
group-name	The load balance group to be operated.
ap-name	The name of the AP to be removed from the balance group.

【Default Configuration】 N/A

【Command Mode】 AC configuration mode

【Default Level】 15

【Usage Guide】 N/A

【Configuration Example】 1: Remove the AP named ap1 from the balance group test-group.

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# num-balance-group del test-group ap1
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.23 num-balance-group enable

Configure the start threshold of the balance group through the num-balance-group enable command. Only when the number of users currently.

associated with the AP reaches the threshold, the quantity load balancing function is activated.

num-balance-group enable group-name number

The load threshold of the restoration balance group is Default Configuration.

no num-balance-group enable group-name number

【Parameter Description】

Parameter	Description
group-name	The name of the load balancing group to be operated.
number	The start threshold of the equalization group, the default is 3, and the range is 0-10, where 0 means that the equalization group does not enable the quantity equalization function.

【Default Configuration】 Start threshold is 3

【Command Mode】 AC configuration

【Default Level】 15

【Usage Guide】 N/A

【Configuration Example】 1: Configure the threshold of the balance group named test-group to 1.

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# num-balance-group enable test-group 1
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.24 num-balance-group mode

Use the num-balance-group mode command to configure the load balance mode of the balancing group.

num-balance-group mode group-name { radio-mode | ap-mode }

Use the no command to restore to Default Configuration.

no num-balance-group mode group-name

【Parameter Description】

Parameter	Description
group-name	The name of the load balancing group to be operated.
radio-mode	Configure the balance group as radio-based load balance.
ap-mode	Configure the balance group as ap-based load balance.

【Default Configuration】 The default is load balance based on AP。

【Command Mode】 AC configuration mode

【Default Level】 15

【Usage Guide】N/A

【Configuration Example】 1: Configure the load balancing mode of the balancing group named test-group as radio-based load balance:

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# num-balance-group mode test-group radio-mode
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.25 num-balance-group num

Configure the load threshold of the balance group.

num-balance-group num group-name number

Restore the load threshold of the balance group to the default value.

no num-balance-group num group-name number

【Parameter Description】

Parameter	Description
group-name	The name of the load balancing group to be operated.
number	The threshold of the equalization group, the default is 3, the range is 0-20, where 0 means that the equalization group does not enable the quantity equalization function.

【Default Configuration】 Threshold is 3

【Command Mode】 AC configuration mode

【Default Level】 15

【Usage Guide】 N/A

【Configuration Example】 1: Configure the threshold of the balance group named test-group to 1.

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# num-balance-group num test-group 1
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.26 package

Create a terminal package and enter the terminal package configuration mode.

package pkg-name

The user can use the no option of this command to delete the specified terminal package configuration.

no package [pkg-name]

【Parameter Description】

Parameter	Description
pkg-name	Terminal package name, length [1,32].

【Default Configuration】 No terminal package configuration

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】 A maximum of 300 terminal packages can be configured on the AC. If the upper limit is exceeded, an error message will be issued.

【Configuration Example】 1: Configure a terminal package named "AAA".

```
AC-FS(config)#package AAA
AC-FS(config-package)#
```

2: Delete the terminal package named "AAA".

```
AC-FS(config)# no package AAA
The opreration will clear package(s) configuration, which may cause corresponding STAs offline . Continue? [no]y
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.27 prevent-jitter

Configure the anti-shake time for offline WLAN users.

prevent-jitter {enable | time keep-time}

The user can use the no option of this command to cancel the anti-shake, or restore the default value of the anti-shake time.

no prevent-jitter {enable | time}

【Parameter Description】

Parameter	Description
enable	Turn on or off STA anti-shake of WLAN.
time	Configure anti-shake time (default is 60s).
keep-time	The number of seconds for STA anti-shake, the value range is 1-86400.

【Default Configuration】 None

【Command Mode】 WLAN configuration mode

【Default Level】 15

【Usage Guide】 After the user anti-shake function is enabled, the STA under the WLAN will remain online for a period of time after disassociating, the default is 60s. During this period, if the user goes online again on the same WLAN of the AP, it's never offline;
If the user associates with the same WLAN of other APs, it is treated as roaming; if it is associated with other WLANs, it is treated as switching WLAN.
Note: When the user is actively kicked offline from the device or authentication server, the anti-shake will not take effect and the STA will immediately go offline.

【Configuration Example】 1: Enable the anti-shake function for Wlan 1.

```
AC-FS(config)#wlan-config 1

AC-FS(config-wlan)#prevent-jitter enable
```

2: Configure the anti-shake time of Wlan 1 to 300s.

```
AC-FS(config)#wlan-config 1

AC-FS(config-wlan)#prevent-jitter time 300
```

3: Cancel the anti-shake function of Wlan 1.

```
AC-FS(config)#wlan-config 1

AC-FS(config-wlan)#no prevent-jitter enable
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.28 primary-STA

Configure the main STA in a STA package.

primary-sta mac-address

The user can use the no option of this command to delete the main STA configuration in the specified STA package.

no primary-sta

【Parameter Description】

Parameter	Description
mac-address	The MAC address of the main STA, in the format H.H.H.

【Default Configuration】 N/A

【Command Mode】 Station package configuration mode

【Default Level】 15

【Usage Guide】Only one main STA is allowed to be configured in a station package, therefore, when using this command to configure the main STA in the station package, if the main STA in the terminal package already exists, it will be directly overwritten.

【Configuration Example】 1: Configure the main STA with the MAC address 00d0.f800.0001 for the station package "AAA".

```
AC-FS(config)#package AAA
AC-FS(config- package)#primary-sta 00d0.f800.0001
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.29 secondary-STA

Configure the slave STA in a station package.

secondary-sta mac-address

The user can delete the slave STA configuration in the specified station package with the no option of this command.

no secondary-sta [mac-address]

【Parameter Description】

Parameter	Description
mac-address	The MAC address of the slave STA, the format is like H.H.H

【Default Configuration】 N/A

【Command Mode】 Station package configuration mode

【Default Level】 15

【Usage Guide】A station package allows up to 100 slave STA to be configured. When using this command to configure the secondary STA, if the specified secondary STA already exists, an error message will be displayed; If the total number of slave STA in the station

package has reached 100, a corresponding error prompt will be given.

【Configuration Example】 1: Configure the MAC address of STA from 00d0.f800.0002 in the station package "cart 1".

```
AC-FS(config)#package cart 1
AC-FS(config- package)#secondary-sta 00d0.f800.0002
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.30 show ac-config client

Display the information of all connected STA on this AC.

show ac-config client [by-ap-name | 802.11a | 802.11b | 802.11n | 802.11g | 802.11ac | other]

【Parameter Description】

Parameter	Description
by-ap-name	Sort by AP's name.
802.11a	Display 802.11a user information.
802.11b	Display 802.11b user information.
802.11n	Display 802.11n user information.
802.11g	Display 802.11g user information.
802.11ac	Display 802.11ac user information.
other	Display unknown user information.

【Command Mode】 Privileged Mode

【Default Level】 1

【Usage Guide】N/A

【Configuration Example】 1: Display the information of all connected STA on this AC.

```
AC#show ac-config client
========= show sta status ========= AP :  ap name/radio id
Status:  Speed/Power Save/Work Mode/Roaming State, E = enable power save, D = disable power save

Total Sta Num :  1
STA MAC          IP Address       AP                          Wlan Vlan Status Asso Auth Link Auth Up time

78e4.00d3.1183 192.168.248.2 te/1                                  1    1..... 65.0M/D/bn
Open       Open      0: 00: 08: 10
```

【Prompt Information】 -

【Platform Description】 AC

2.31 show ac-config client detail

Display the detailed information of the specified wireless user.

show ac-config client detail mac-address

【Parameter Description】

Parameter	Description
mac-address	MAC address of wireless user.

【Command Mode】 Privileged Mode

【Default Level】 1

【Usage Guide】 N/A

【Configuration Example】 1: Display the information of all connected STA on this AC.

```
AC#show ac-config client
========= show sta status ========= AP :    ap name/radio id
Status:    Speed/Power Save/Work Mode/Roaming State, E = enable power save, D = disable power save

Total Sta Num :    1
STA MAC          IP Address        AP                        Wlan Vlan Status Asso Auth Link Auth Up time

78e4.00d3.1183 192.168.248.2 te/1                                    1     1      65.0M/D/bn
Open        Open       0: 00: 08: 10
```

【Prompt Information】 -

【Platform Description】 AC

2.32 show ac-config client hot-backup

Display backup information of wireless users.

show ac-config client hot-backup

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged Mode

【Default Level】 1

【Usage Guide】 N/A

【Configuration Example】 1: Display backup information of wireless users.

```
AC# show ac-config client hot-backup

STA MAC          IPV4 Address      Context Name                    Status AC DESCRIPTION
```

【Prompt Information】 -

【Platform Description】 AC

2.33 show ac-config client statistic

Shows the number of online/offline times and roaming times of wireless users in different time periods in the past.

show ac-config client statistic

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged Mode

【Default Level】 1

【Usage Guide】 N/A

【Configuration Example】 1: Display statistics of specified wireless users.

```
 AC# #show ac-config client statistic

========= show sta statistic ========= STA online times in 5 second:    13

STA offline times in 5 second:    10 STA roaming times in 5 second:    2

STA online times in 1 minute:    30 STA offline times in 1 minute:    25 STA roaming times in 1 minute:    10

STA online times in 1 hour:    200 STA offline times in 1 hour:    300 STA roaming times in 1 hour:    100

Maxinum rate of STA-online in 1 hour:    20/s
```

【Prompt Information】 -

【Platform Description】 AC

2.34 show ac-config flow-balance summary

This command is used to view the detailed configuration information of a traffic-based load balance group.

show ac-config flow-balance summary

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged Mode

【Default Level】 1

【Usage Guide】 N/A

【Configuration Example】 1: View detailed configuration information of a traffic-based load balance group:

```
AC-FS(config)#show ac-config flow-balance summary
Group        Threshold    AP NAME
-------------------------------------------------------------------------------
test-group1        5*100kbps ap1,ap2,ap3 test-group2        6*200kbps ap4,ap5,ap6
```

【Prompt Information】 -

【Platform Description】 AC

2.35 show ac-config num-balance summary

This command is used to view the detailed configuration information of a quantity-based load balancing group.

show ac-config num-balance summary

【Parameter Description】

Parameter	Description

-	-

【Command Mode】 Privileged Mode

【Default Level】 1

【Usage Guide】 N/A

【Configuration Example】 1: View detailed configuration information of a quantity-based load balancing group:

```
AC-FS(config)#show ac-config num-balance summary Group        Threshold AP NAME
_________________ ___________ ___________________________
                  test-group1        1          ap1,ap2,ap3
```

【Prompt Information】 -

【Platform Description】 AC

2.36 show assoc-control

Display the current running status of the associated control.

show assoc-control

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged Mode

【Default Level】 1

【Usage Guide】 None

【Configuration Example】 1: Display the current running status of the associated control.

```
AC-FS# show assoc-control
Association control is enabled.
```

2: Display the current running status of the associated control.

```
AC-FS# show assoc-control
Association control is disabled.
```

【Prompt Information】 -

【Platform Description】 AC

2.37 show control-zone

Display the configuration information of the associated control domain.

show control-zone [summary | czone-name]

【Parameter Description】

Parameter	Description
summary	Show summary information.
czone-name	The name of the associated control domain to be viewed, length [1,64].

【Command Mode】 Privileged Mode

【Default Level】 1

【Usage Guide】 Use the show control-zone summary command to view the configured associated control zone information, use show control-zone or show control-zone czone-name to view related control zone information, view AP information in the control domain.

【Configuration Example】 1: Display all associated control domain information.

```
AC-FS# show control-zone summary control zone num :  4

Grade 1 Class 1

Grade 1 Class 2

Grade 1 Class 3

Grade 2 Class 1
```

2: Display all associated control domain information.

```
AC-FS# show control-zone summary

No control zone configuration.
```

3: Display detailed configuration information of all associated control domains.

```
AC-FS# show control-zone control zone num :  3 control-znoe AP

Grade 1 class 1          AP1(1)-1 00d0.f800.889f

 AP1(1)-2 00d0.f800.7869

Grade 2 class 2          AP2(2)-1 00d0.f800.889f

Grade 2 class 3              AP2(3)-1 offline

Grade 3 class 3              n/a
```

4: Display detailed configuration information of all associated control domains.

```
AC-FS# show control-zone

No control zone configuration.
```

5: Display the detailed configuration information of the associated control domain named "grade 1 class 1".

```
AC-FS# show control-zone grade 1 class 1
control-zone          AP
_____________         ____________________________
Grade 1 Class 1       AP1(1)-1 00d0.f800.889f
                          AP1(1)-2 00d0.f800.7869
Grade 2 Class 2       AP2(2)-1 00d0.f800.889f
Grade 2 Class 3       AP2(3)-1 offline
Grade 2 Class 3       n/a
```

6: Display the detailed configuration information of the associated control domain named "grade 5 class 1".

```
AC-FS# show control-zone grade 5 class 1
No such control zone configuration.
```

【Prompt Information】 -

【Platform Description】 AC

2.38 show package

Display terminal package configuration information.

show package [pkg-name]

【Parameter Description】

Parameter	Description
pkg-name	The name of the station package to be viewed, length [1,32].

【Command Mode】 Privileged Mode

【Default Level】 1

【Usage Guide】 N/A

【Configuration Example】 1: Show all station package configurations.

```
AC-FS# show package total package num :  2
========== package_1 ========== primary STA :  none
secondary STA num :  0
primary STA :  00d0.f809.0092 secondary STA num :  4 00d0.f809.0096
00d0.f809.0097
0          0d0.f809.0098
00d0.f809.0099
```

2: Show all station package configurations.

```
AC-FS# show package
No package configuration.
```

【Prompt Information】 -

【Platform Description】 AC

2.39 show STA-blacklist

Show STA blacklist.

show sta-blacklist

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged Mode

【Default Level】 1

【Usage Guide】 N/A

【Configuration Example】 1: STAs in the current STA blacklist.

```
AC-FS#show sta-blacklist
Num          STA MAC          Add time
_____  _____  _____
1            0080.1111.1111 2013-07-02 13: 56: 22
2            0090.2222.3333 2013-07-02 13: 56: 35
3            0070.1111.2233 2013-07-02 13: 57: 08
```

【Prompt Information】 -

【Platform Description】 AC

2.40 STA-balance num-limit enable

Configure to enable STA to automatically stop the load balance function after multiple association failures.

sta-balance num-limit enable

The load balancing function can be automatically stopped by using the no prefix of this command.

no sta-balance num-limit enable

【Parameter Description】 -

【Default Configuration】 By default, this function is turned off

【Command Mode】 AC configuration mode

【Default Level】 15

【Usage Guide】 In the default mode, the STA will always try to connect to the AP obtained from the load balancing result. With the sta-balance function enabled, STA can try to connect to the same AP at most 5 times under load balancing. If all connections fail for 5 times, then the next connection to the STA will not be restricted by load balance.

【Configuration Example】 1: Enable sta-balance function.

```
AC-FS(config)# ac-controller
AC-FS(config-ap)# sta-balance num-limit enable
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.41 STA-blacklist

sta-blacklist command can be used to configure the STA blacklist function on and off, at the same time, the aging time of the STA in the blacklist can be configured, In addition, detect-time and fail-limit can be configured to define whether STA is the source of the attack.

sta-blacklist { enable | lifetime | detect-time | fail-limit } [seconds | number]

sta-blacklist command can be used to configure the disable of the STA blacklist function through the no parameter, at the same time, the aging time of the STA in the blacklist can be configured.

In addition, detect-time and fail-limit can be configured to define whether STA is the source of the attack.

no sta-blacklist { enable | lifetime | detect-time | fail-limit } [seconds | number]

【Parameter Description】

Parameter	Description
enable	Enable STA blacklist function.
lifetime	Indicates the aging time of the STA in the blacklist.
detect-time	Represents detection time, and the STA is listed as the suspect attack end at the first failure, if at detection blacklist sta lists the maximum number of STA association failures (i. e. fail-limit);
fail-limit	Show the upper number of STA association failures in the detect-time time.
seconds	For time, lifetime | detect-time option parameters, in seconds, for lifetime when takenValues range 60-1200, indicating the value range 5-60 for detect-time.
number	Indicates the number of STA launch failures, the fail-limit option parameter, with a configuration range of 1-100.

【Default Configuration】 The blacklist function is turned off by default, the lifetime default is 300 seconds, the detect-time default is 60 seconds, and the number default value is 5.

【Command Mode】 AC configuration mode

【Default Level】 15

【Usage Guide】 N/A

【Configuration Example】 1: Open the STA blacklist function.

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# sta-blacklist enable
```

2: Turn off the STA blacklist function.

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# no sta-blacklist enable
```

3: Configure the blacklist aging time.

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# sta-blacklist lifetime 60
```

4: Configure the detection time.

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# sta-blacklist detect-time 10
```

5: Configure association failed upper limit.

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# sta-blacklist fail-limit 20
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.42 STA-idle-timeout

User can set the aging time for the wireless users in the specified AP or AP group through the sta-idle-timeout.

sta-idle-timeout timer-num

The client timeout timer attribute can be restored to the default value with the no prefix of the command.

no sta-idle-timeout

【Parameter Description】

Parameter	Description
timer-num	To set the aging time value, in seconds, take the value range: 60 to 86400 Description: The vale steps in 15 seconds, and the configuration value moves automatically if not 15 integer times.

【Default Configuration】 By default, the timer is 300s.

【Command Mode】 AP configuration mode or AP group configuration mode

【Default Level】 15

【Usage Guide】 If no information is received from the wireless user within the set time, the wireless user will be considered to leave the WLAN network and the system removes it from the network.

【Configuration Example】 1: Enter the configuration mode of AP0001 and its client timeout timer time is 600s.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# sta-idle-timeout 600
```

2: Enter the configuration mode of the AP0001 and configure its client timeout timer time back to the default value of 300s.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# no sta-idle-timeout-timer
```

3: Enter the default AP group and configure its client timeout timer time to 600s.

```
AC-FS(config)# ap-group default
AC-FS(config-group)# sta-idle-timeout 600
```

4: Enter the default AP group, and configure its client timeout timer time to recover to the default value of 300s.

```
AC-FS(config)# ap-group default
AC-FS(config-group)# no sta-idle-timeout-timer
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.43 STA-limit

The maximum number of connected wireless users can be configured by sta-limit, globally in AC configuration mode, or in AP group and AP configuration mode, or the maximum number of WLAN connected wireless users in WLAN configuration mode.

sta-limit client-num

The default values can be recovered in the no form.

no sta-limit

【Parameter Description】

Parameter	Description

client-num	Maximum number of connected wireless users. AC Configuration mode: the maximum is 32 times the number of AP supported by AC (limited by license). AP Group configuration mode: the maximum value is 1536. AP configuration mode: the maximum value of the offline AP or ap-config all is 1536, and the online AP maximum is determined based on the model of the AP. The WLAN configuration mode: the maximum value is the same as in the AC configuration mode.

【Default Configuration】 AC Configuration mode: The default is 32 times the number of AP supported by AC (limited by license) In AP group configuration mode: the default is 64. AP configuration mode: the default value of offline AP or ap-config all is 64, and the default value of online AP is determined in WLAN configuration mode according to the model of AP: the default is not limited.

【Command Mode】 AC configuration mode, AP group configuration mode, AP configuration mode, WLAN configuration mode

【Default Level】15

【Usage Guide】 Configure how many clients the device can provide services at most. The value should not exceed the maximum supported by the AC and the maximum value of the license limit. Different AC products support different maximum number of wireless users.

For the configuration of ap-config all, ap-group and offline AP, the allowed user's configuration range is 1~512. If the user-configured value exceeds the AP

The actual number of STAs that can be supported. When the AP goes online, it will be automatically adjusted to the actual maximum number of STAs that can be supported. For online AP configuration, the maximum value configurable by this command is the maximum value actually supported by the AP.

【Configuration Example】1: Configure the AC to serve up to 2400 clients.

```
AC-FS(config-ac)# sta-limit 2400
```

2: Configure the maximum number of wireless users allowed to join by all APs in the AP group (Default) to 20.

```
AC-FS(config)# ap-group default
AC-FS(config-group)# sta-limit 20
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.44 STA-limit per-ap

With the sta-limit per-ap, you can configure the maximum number of connected wireless users per AP under the WLAN.

sta-limit per-ap client-num

The default values can be recovered in the no form.

no sta-limit per-ap

【Parameter Description】

Parameter	Description
client-num	Maximum number of connected wireless users. Value range: 1-1536.

【Default Configuration】 There are no restrictions imposed by default.

【Command Mode】 WLAN configuration mode

【Default Level】15

【Usage Guide】 Configure the number of supported users per AP under that WLAN. If the configuration value exceeds the maximum limit of AP, the maximum limit prevail.

【Configuration Example】 1: Only 10 user associations are allowed under WLAN 1 for each AP.

```
AC-FS(config)# wlan-config 1

AC-FS(config-wlan)# sta-limit per-ap 10
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.45 STA-limit radio

The maximum number of connected wireless users can be configured with the sta-limit, and the maximum number of radio accessible wireless users on an AP can be specified in the AP group and AP configuration mode.

sta-limit client-num radio radio-id

The default values can be recovered in the no form.

no sta-limit radio radio-id

【Parameter Description】

Parameter	Description
client-num	Maximum number of connected wireless users, value range: 1-156 (or AP capacity).
radio-id	radio logo.

【Default Configuration】 There are no limitations to default.

【Command Mode】 AP group configuration mode, AP configuration mode

【Default Level】 15

【Usage Guide】 The user number limit in the sta-limit radio command has no dependence on the user number limit in the sta-limit. That is, the user number limit in sta-limit radio can be greater than the user number limit configured in sta-limit.

For ap-config all, ap-group, and offline AP configurations, you allow users' configurations to range from 1 to 156. If the user configured value exceeds AP. The number of STA that can actually be supported by the radio is automatically adjusted to the maximum STA actually supported when the AP is online. For the configuration of an online AP, the maximum value configurable by the command is the maximum actually supported by the radio on the AP.

【Configuration Example】 1: The maximum number of wireless users allowed on the radio 1 with a configured AP is 20.

```
AC-FS(config)# ap-config ap1
AC-FS(config-ap)# sta-limit 20 radio 1
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.46 STA-logging rate-limit

The sta-logging rate-limit can configure the maximum syslog output per second, and this syslog includes the STA offline as well as the syslog for the STA information changes.

sta-logging rate-limit limit-num

The default number of syslog output bars per second can be recovered in the no form.

no sta-logging rate-limit

【Parameter Description】

Parameter	Description
limit-num	For the syslog of STA, the maximum number of output per second. Range of values: 0-10,000.

【Default Configuration】 The default output is up to 5 pieces per second.

【Command Mode】 AC configuration mode

【Default Level】 15

【Usage Guide】 N/A

【Configuration Example】 1: The maximum number of bars per second for the configuration to output the syslog is 100.

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# sta-logging rate-limit 100
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

2.47 STA-logging mac-fmt-line

Through sta-logging mac-fmt-line, you can configure the syslog format output when sta gets an IP online.

sta-logging mac-fmt-line

The default syslog format can be restored via the no form.

no sta-logging mac-fmt-line

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 None

【Command Mode】 AC configuration mode

【Default Level】 15

【Usage Guide】 The default sta goes online to get the IP when the output syslog format is: User Online, MAC Address 0001.2fe1.5022, AP Name name, base radio MAC: 0074.9c5b.288a, IP address 192.168.1.1, SSID; AC-FS the syslog format after the configuration command is: CLIENT_ONLINE: UserIP=192.168.1.1, UserMAC=00-01-2F-E1-50-22, APMAC=00-74-9C-5B-28-85.

【Configuration Example】 1: Configure the syslog format to output when the sta goes online to get the IP.

```
AC-FS(config)# ac-controller

AC-FS(config-ac)# sta-logging mac-fmt-line
```

【Verification】 -

3 STAMG Station Access Control List

3.1 blacklist mac

Add terminal to the complete machine / AP / SSID blacklist, and the mnemonic is used to identify the terminal for easy user access.

blacklist mac sta-mac [in-ap ap-mac | in-ssid ssid-string] [mnemonic string]

The user can delete the terminal with the no option of the command.

no blacklist mac sta-mac [in-ap ap-mac | in-ssid ssid-string]

【Parameter Description】

Parameter	Description
sta-mac	The MAC address of wireless user, MAC address without parameters is the configuration machine blacklist.
in-ap ap-mac	After configAP-based blacklist, the terminal cannot be associated with this AP, only this parameter on AC.
in-ssid ssid-string	After configuring an SSID-based blacklist, the terminal cannot be associated with this SSID.
string	Mnemonic, show command viewing is displayed for easy user access.

【Default Configuration】 By default, no station is on the blacklist.

【Command Mode】 Station control list configuration mode

【Default Level】 15

【Usage Guide】 The station is not allowed to access after the blacklist is configured. MAC black and white list is mutually exclusive, the STA MAC joining the white list can not join the blacklist if the station online will kick offline.

【Configuration Example】 1: Add the station to the whole machine blacklist:

```
AC-FS(black-white-list)#blacklist mac 0025.9cb3.fd2c mnemonic test
```

2: Remove the station from the complete machine blacklist:

```
AC-FS(black-white-list)#no blacklist mac 0025.9cb3.fd2c
```

【Verification】 show black-white-list blacklist [in-ap ap-mac | in-ssid ssid-string] confirm the station added to the blacklist.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC, Fat AP

3.2 black-white-llist

Enter the station access control list setting mode.

black-white-list

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 N/A

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】 -

【Configuration Example】 Enter the station access control list setting mode:

```
AC-FS(config)# black-white-list

AC-FS(black-white-list)#
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC, Fat AP

3.3 export

Export the terminal control list configuration to a file.

Export

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 N/A

【Command Mode】 Station control list configuration mode

【Default Level】 15

【Usage Guide】 Export the current configuration to the black-white-list.csv, and the path is / data /.

【Configuration Example】 Export the configuration to the black-white-list.csv:

```
AC-FS(black-white-list)#export
```

【Verification】 The exported file is found by dir; the more command views the file contents.

【Prompt Information】 Export the number of successful table items.

【Common Mistake】 The Flash space may not be enough to save the exported profile to print the prompt.

【Platform Description】 AC, Fat AP

3.4 import

Import stationl control list configuration from a file.

import filename {replace | append}

【Parameter Description】

Parameter	Description
filename	The file name to import can contain a path, and the default path is / data /.
replace	Override the current configuration with an import configuration.
append	Mides the import configuration with the current configuration.

【Default Configuration】 N/A

【Command Mode】 Station control list configuration mode

【Default Level】 15

【Usage Guide】Selecting replace overrides the current configuration with the import configuration

Choosing append merges the import configuration and the current configuration.

【Configuration Example】 1. Import a configuration from the black-white-list.csv file that overrides the current configuration:

```
AC-FS(black-white-list)#import black-white-list replace
```

2. Import a configuration from the black-white-list.csv file to merge the import configuration with the current configuration:

```
AC-FS(black-white-list)#import black-white-list append
```

【Verification】 show black-white-list config can check the current configuration.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC, Fat AP

3.5 reset blacklist

Empty the complete machine / AP / SSID blacklist.

reset blacklist [in-ap ap-mac | in-ssid ssid-string]

【Parameter Description】

Parameter	Description
-	Reset blacklist without parameters is to clear the blacklist of the whole machine.
in-ap ap-mac	Empty the AP-based blacklist, only this parameter on AC.
in-ssid ssid-string	Clear SSID-based blacklist.

【Default Configuration】 N/A

【Command Mode】 Station control list configuration mode

【Default Level】 15

【Usage Guide】 -

【Configuration Example】 Empty the whole machine blacklist:

```
AC-FS(black-white-list)#reset blacklist
```

【Verification】 show black-white-list black [in-ap ap-mac | in-ssid ssid-string] can check the terminals added to the blacklist.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC, Fat AP

3.6 reset whitelist

Empty the complete machine / AP / SSID whitelist

reset whitelist [vendor] [in-ap ap-mac | in-ssid ssid-string]

【Parameter Description】

Parameter	Description
-	Reset whitelist without parameters is to clear the whitelist of the whole machine.
vendor	The OUI whitelist keyword, representing the operation of the OUI whitelist.
in-ap ap-mac	Empty the AP-based whitelist with this parameter on AC.
in-ssid ssid-string	Clearance whitelist based on SSID.

【Default Configuration】 N/A

【Command Mode】 Station control list configuration mode

【Default Level】 15

【Usage Guide】-

【Configuration Example】 Empty the complete machine white list:

```
AC-FS(black-white-list)#reset whitelist
```

【Verification】 show black-white-list white [vendor] [in-ap ap-mac | in-ssid ssid-string] can check the terminals added to the whitelist.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC, Fat AP

3.7 show black-white-list

View the status and configuration of the access control black and white list, etc.

show black-white-list {summary | config | conflict | sta-mac sta-mac | blacklist [in-ap ap-mac | in-ssid ssid-string] | whitelist [vendor] [in-ap ap-mac | in-ssid ssid-string]}

【Parameter Description】

Parameter	Description
summary	Displays the basic information of the stationl control list, such as the enabling status and the number of table items.
config	Displays the complete configuration of the station control list.
conflict	Displays the station both in the black and white list.
sta-mac sta-mac	Displays the configuration location of a specific station.
blacklist	Displays the complete machine blacklist list items and mnemonic characters.
blacklist in-ap ap-mac	Displays AP Blacklist table items and mnemonic, only on AC.
blacklist in-ssid ssid-string	Displays is based on SSID Blacklist table items and mnemonics.

whitelist	Displays the complete machine whitelist items and mnemonics.
summary	Displays the basic information of the stationl control list, such as the enabling status and the number of table items.
config	Displays the complete configuration of the station control list.
conflict	Displays the station both in the black and white list.
sta-mac sta-mac	Displays the configuration location of a specific station.
blacklist	Displays the complete machine blacklist list items and mnemonic characters.

【Default Configuration】 -

【Command Mode】 Privilege mode

【Default Level】 15

【Usage Guide】 -

【Configuration Example】 View the complete configuration of the station control list:

```
AC-FS(black-white-list)#show black-white-list config
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AP, Fat AP

3.8 whitelist mac

Add the terminal to the whitelist of the whole machine/AP/SSID, the mnemonic is used to identify the identity of the station, which is convenient for users to check.

whitelist mac sta-mac [in-ap ap-mac | in-ssid ssid-string] [mnemonic string]

The user can delete the terminal with the no option of the command.

no whitelist mac sta-mac [in-ap ap-mac | in-ssid ssid-string]

【Parameter Description】

Parameter	Description
sta-mac	MAC address of wireless user with no parameters behind sta-mac.
in-ap ap-mac	Configure an AP-based whitelist, which only on AC.
in-ssid ssid-string	Configuration based on SSID.
string	Mnemonic, show command viewing is displayed for easy user access.

【Default Configuration】 No terminal join the whitelist by default.

【Command Mode】 Terminal control list configuration mode

【Default Level】 15

【Usage Guide】 Users joining the whitelist allow access,the MAC black and white lists are mutually exclusive, and the STA MAC on the blacklist cannot be added to the whitelist.

【Configuration Example】 1: Add the terminal to the whole machine white list:

```
AC-FS(black-white-list)#whitelist mac 0025.9cb3.fd2c mnemonic test
```

2: Remove the stationl from the complete machine whitelist:

```
AC-FS(black-white-list)#no whitelist mac 0025.9cb3.fd2c
```

【Verification】 show black-white-list whitelist [in-ap ap-mac | in-ssid ssid-string] can check the terminals added to the whitelist.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC, Fat AP

3.9 whitelist vendor mac

Add a terminal to the OUI white list of the complete machine / AP / SSID with the mnemonic used to identify the terminal for user access.

whitelist vendor mac sta-oui [in-ap ap-mac | in-ssid ssid-string] [mnemonic string]

The user can delete the terminal with the no option of the command.

no whitelist vendor mac sta-oui [in-ap ap-mac | in-ssid ssid-string]

【Parameter Description】

Parameter	Description
sta-oui	The OUI address of the wireless user is in the format hhhh.hh with no parameters behind sta-oui.
in-ap ap-mac	Configure an AP-based OUI whitelist, with this parameter only on the AC.
in-ssid ssid-string	Configure the SSID-based OUI whitelist.
string	Mnemonic, show command viewing is displayed for easy user access.

【Default Configuration】 By default no terminal join the OUI whitelist.

【Command Mode】 Station control list configuration mode

【Default Level】 15

【Usage Guide】 The OUI whitelist matches the station OUI address, and the terminal of the OUI whitelist allows access; The blacklist has a higher priority than the OUI whitelist and is not allowed to access when the station is in the black and white list at the same time.

【Configuration Example】 1: Add the station to the complete machine OUI white list:

```
AC-FS(black-white-list)#whitelist vendor mac 0025.9c mnemonic test
```

2: Remove the station from the complete machine OUI whitelist:

```
AC-FS(black-white-list)#no whitelist vendor mac 0025.9c
```

【Verification】 show black-white-list whitelist [vendor] [in-ap ap-mac | in-ssid ssid-string] can check the terminals added to the whitelist.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC, Fat AP

4 CAPWAP

4.1 ac-domain-name

Configure the domain name for the AP Discovery AC.

ac-domain-name ac-domain-name

Restore the Default Configuration.

no ac-domain-name

【Parameter Description】

Parameter	Description
ac-domain-name	Configure the domain name of AP Discovery AC, configured up to 64 characters and cannot contain spaces.

【Default Configuration】 By default, the ac.AC-FS.com.cn

【Command Mode】 AP configuration mode or AP group configuration mode

【Default Level】 15

【Usage Guide】 AP can discover AC through the DNS domain name. With this command, you can modify the domain name of AP discovery AC, so that different AP can discover different AC through different domain domains.

【Configuration Example】 The domain name for the configuration AP Discovery AC is AC-FS-ac.

```
AC-FS(config-ap)# ac-domain-name AC-FS-ac
```

【Verification】 Use the show ap-config cb ap-name command to see if the configuration is successful.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

4.2 ac-domain-name

Configure the domain name for the AP Discovery AC.

ac-domain-name ac-domain-name

Restore the Default Configuration.

ac-domain-name

【Parameter Description】

Parameter	Description
ac-domain-name	Configure the domain name of AP Discovery AC, configured up to 64 characters and cannot contain spaces.

【Default Configuration】 By default,ac.AC-FS.com.cn

【Command Mode】 AP configuration mode or AP group configuration mode

【Default Level】 15

【Usage Guide】 AP can discover AC through the DNS domain name. With this command, you can modify the domain name of AP discovery AC, so that different AP can discover different AC through different domain domains.

【Configuration Example】 1: The domain name for the configuration AP Discovery AC is AC-FS-ac.

```
AC-FS(config-ap)# ac-domain-name AC-FS-ac
```

【Verification】 Use the show ap-config cb ap-name command to see if the configuration is successful.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 Only the AC supports this command.

4.3 ac-ip- ipv4

Configure the AP to join the specified AC.

acip ipv4 ip-address [ip-address…]

Delete the specified AC configuration.

no acip ipv4

【Parameter Description】

Parameter	Description
ip-address	Static IP addresses, you can configure up to 6 static addresses.

【Default Configuration】 -

【Command Mode】 The AP global configuration mode or the AP configuration mode of the AC.

【Default Level】 15

【Usage Guide】 Thin AP is generally of zero configuration, and AC can be found through broadcast, multicast, DHCP, and DNS, AC can also be added through a statically configured AC address. By configuring this command, the AP sends discovery request messages to these IP addresses to probe the validity of the AC, and then select an AC to join.

【Configuration Example】 1: The static address list to adding AC for thin AP is 192.168.1.1,192.168.2.1.

```
AC-FS(config)# acip ipv4 192.168.1.1 192.168.2.1
```

2: The static address list for configuring the AP0001 to join the AC is 192.168.1.1,192.168.2.1.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# acip ipv4 192.168.1.1 192.168.2.1
```

【Verification】 Fit AP uses the show running-config command, and AC uses show ap-config running to see if the configuration is successful.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

4.4 active-bin-file

Activate an AP software version on the AC, and only the activated AP software version can be used for upgrade.

active-bin-file filename [rgos10]

Delete the relevant configuration.

no active-bin-file filename [rgos10]

【Parameter Description】

Parameter	Description
filename	File name, which can contain the path prefix, and the path prefix includes flash: , tmp: , usb0: , sata0: , The path prefix is followed by the real file name, with a maximum length of 64 bytes.
rgos10	Activate the intermediate version of rgos10 system to rgos11 system, only for the software version of AP.

【Default Configuration】 -

【Command Mode】 AC configuration mode

【Default Level】 15

【Usage Guide】 AC needs to activate the version file when upgrading the download AP. Due to the large difference between rgos10 system and rgos11 system, rgos10 keywords is required to upgrade with the release rgos10 to rgos11.

Only the bin is loaded into memory when the AP needs to upgrade. This part is automatically uninstalled from memory when there is no AP to upgrade.

The software version already exists in the AC system file before configuring the command.

 To delete the version file after activating the version file, you need to delete the configuration to remove the occupancy of the version file, otherwise there will be an error when deleting the file.

 The direct overwrite version file cannot trigger the AP upgrade and requires reactivation of the version file.

【Configuration Example】 1: Activate an AP software version file on the AC: ap.bin.

```
AC-FS(config-ac)# active-bin-file ap.bin
```

2: Activate an AP software version file on the AC: ap.bin,the software version is in the usb0: File system.

```
AC-FS(config-ac)# active-bin-file usb0: ap.bin
```

3: Delete an AP software version file that is activated on the AC: ap.bin.

```
AC-FS(config-ac)# no active-bin-file ap.bin
```

【Verification】 Use the show ac-config active-file to view the activated software version.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

4.5 ap-image

Configure the AC upgrade to upgrade the AP of the specified series using the specified file. This command will work on all APs connected to this AC.

ap-image { auto-upgrade | filename serial-name }

Unconfigure.

no ap-image { auto-upgrade | filename serial-name }

【Parameter Description】

Parameter	Description
auto-upgrade	Automatically match the AP model applicable to the software version to upgrade.
filename	Specifies the software version name, including the suffix. The file name is the same as the file name specified by the active-bin-file command.
serial-name	The AP model series that will be upgraded.

【Default Configuration】 -

【Command Mode】 AC configuration mode

【Default Level】15

【Usage Guide】 For AP version upgrade, you can use the adaptive upgrade option to automatically match the version and upgrade the AP without configuring the corresponding relationship between the product model and software version of the AP. You can also use the specified file to upgrade the specified series of APs. When two upgrade modes, automatic upgrade and upgrade of specified series exist at the same time, the configuration method of the specified series will be preferred for upgrade. When configuring the AC to upgrade the version of the specified AP product series, the three steps of creating the AP product series, configuring the software version corresponding to the specified AP and activating the software version are indispensable.

Adaptive upgrade cannot use the transition version from FSos10 to FSos11 to upgrade the AP of the rgos10 system.

【Configuration Example]】1: Configure the product series named test-serial to upgrade using the ap.bin file.

```
AC-FS(config-ac)# active-bin-file ap.bin
AC-FS(config-ac)# ap-serial test-serial AP220-E hw-ver 1.0
AC-FS(config-ac)# ap-image ap.bin test-serial
```

【[Verification】1: Use the show ac-config serial-product command to view the correspondence between product series, product models, and upgrade versions.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.6 ap-image

Use this command to upgrade a specified AP with a specified file. This command does not support the ap-config all mode. Use the no form of this command to remove the settings.

ap-image filename

unconfigure.

no ap-image

【Parameter Description】

Parameter	Description

filename	Specifies an AP software version filename for upgrade, including the suffix.

【Default Configuration】 N/A

【Command Mode】 AP configuration mode

【Usage Guide】 N/A

【Configuration Examples】 The following example upgrades AP0001 with the file ap.bin.

```
AC-FS(config-ac)# active-bin-file ap.bin
AC-FS(config-ac)# exit
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# ap-image ap.bin
```

【Related Commands】 N/A

【Platform Description】 N/A

4.7 apip ipv4

Use this command to configure a static IP address for a specified AP. Use the no form of the command to remove the configuration.

apip ipv4 ip-addressnetwork-maskgateway

no apip ipv4

【Parameter Description】

Parameter	Description
ip-address	The static IP address.
network-mask	The subnet mask.
gateway	The gateway address.

【Default Configuration】 N/A

【Command Mode】 AP global configuration mode

【Usage Guide】 In general, the fit AP has no configuration. Its IP address and gateway can be dynamically obtained by DHCP. When the CAPWAP tunnel between AP and AC is established, AC delivers the static IP address for AP, so that the address of AP maintains unchanged after AP is rebooted. In special application scenario, you can configure this command in AP global configuration mode to manually set the static IP address for the fit AP.

1. With the AP address configured as static, the DHCP is disabled, and the AC address obtained through the OPTION of DHCP. Therefore, after this command is configured, you need to configure the AC address using the command "acip" on the AP so that the AP can find and join the AC when the AP and the AC are not in the same subnet.

2. The configuration of this command will be automatically saved after the AP configuration. No command of saving is required to be executed.

3. This command serves the same purpose as the command "ip address" on the AC in the AP configuration mode. However, when the AP joins the AC, if the command "ip address" exists in the AP configuration mode of the AC and conflicts with the command "apip", the static address of the AP will be updated and the CAPWAP tunnel will be re-created.

【Configuration Examples】The following example configures the static IP address of the fit AP as 192.168.1.2, the subnet mask as 255.255.255.0, and the gateway as 192.168.1.1.

```
FS(config)# apip ipv4 192.168.1.2 255.255.255.0 192.168.1.1
```

【Verification】1: Use the show running-config command to check whether the configuration is successful.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

```
AC-FS(config-ac)# active-bin-file ap.bin
AC-FS(config-ac)# exit
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# ap-image ap.bin
```

4.8 apip pppoe

Use this command to enable the AP to obtain the address through PPPoE. Use the no form of this command to restore the default setting.

apip pppoe

No apip.

Pppoe

【Parameter Description】

Parameter	Description
N/A	N/A

【Default Configuration】 By default, the PPPoE mode is not specified, and the AP obtains the address through DHCP.

【Command Mode】 AP global configuration mode

【Usage Guide】 After configuring this command, you should perform PPPoE and configure the default route to point to the dialer interface to enable communication between the AP and the AC.

CAPWAP can select only dialer 1 as the source port. Therefore, PPPoE dial requires dialer 1.

【Configuration Examples】 The following example enables the fit AP to obtain the address through PPPoE.

```
AC-FS(config)# apip pppoe
```

-

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

4.9 ap-cfg erps raps-vlan

ERPS single ring configuration.

ap-cfg erps raps-vlan vlan-id ring-port west interface-name1 east interface-name2

Configure RPL link and RPL owner node.

ap-cfg erps raps-vlan vlan-id rpl-port { west | east } rpl-owner

unconfigure.

no ap-cfg erps raps-vlan

【Parameter Description】

Parameter	Description
vlan-id	R-APS VLAN ID
interface-name1	the name of the west port
interface-name2	East port name
west	Specify the port corresponding to west as rpl-owner
east	Specify the port corresponding to east as rpl-owner

【Default Configuration】 Not configured by default, do not use ERPS ring topology.

【Command Mode】 AP global configuration mode.

【Default Level】15

【Usage Guide】 1. During network planning, you need to disconnect a link or shut down a port first, and complete the ring topology after completing the ERPS link configuration.

2. You can find a device in the middle of the ERPS ring to configure the RPL link, so that the traffic can be balanced to the dual uplinks. When one of the links or one device fails, the RPL link of the block will be opened to avoid link failure.

Since the vlan used by ERPS will occupy the vlan capacity of the device, it is required that the vlan cannot use the default vlan of the two smart points + AP, vlan 1 and vlan 2444. Interface-mapping specifies the vlan of sta and wired-vlan specifies that the vlan of the wired port cannot be the same as the vlan of ERPS. Similarly, the vlan of the ap-vlan command cannot be the same as the vlan of the ERPS.

【Configuration Example】1: ERPS single-ring configuration.

```
AC-FS(config)#ap-cfg erps raps-vlan 10 ring-port west gigabitEthernet 0/26 east gigabitEthernet 0/25
```

2: Configure RPL link and RPL owner node

```
AC-FS(config)#ap-cfg erps raps-vlan 10 rpl-port east rpl-ower
```

【Verification】1: Use the show erps command to check whether the configuration is successful.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 This command is only supported by Zhifen+AP host.

4.10 ap-serial

Use this command to configure an AP series on an AC. Only when the AP hardware version and product model are configured to a series can its software version be upgraded through the AC. Use the no form of this command to remove the configuration.

ap-serial serial-name ap-pid1 ap-pid2 ... ap-pidn [hw-ver hardware-version]

Unconfigure.

no ap-serial serial-name

【Parameter Description】

Parameter	Description
serial-name	Indicates an AP series name to be created. The maximum character configuration number is 64, blank space is not included. The maximum number of the AP series that can be supported at the same time: WS5708 series: 16, WS5302 series: 8.
ap-pid1ap-pid2...ap-pidn	Product models
hardware-version	Indicates the AP hardware version, the maximum configuration character is 64, blank space is not included. The hardware version name is a decimal, the mark is 'x' or 'X" which can be used to configure the following character.

【Default Configuration】 N/A

【Command Mode】 AC configuration mode

【Default Level】15

【Usage Guide】 When configuring the AC to upgrade the specified AP product series, create an AP product series, configure the software version corresponding to the specified AP, and activate the software version. These three steps are indispensable, and you need to ensure that the AC system files have been stored before configuration. There is a version of this software.

【Configuration Examples】The following example creates an AP series named test-serial of which the designate AP hardware version is 1.0 on an AC, including these AP models: AP220-SE AP220-SH, AP220-E.

```
AC-FS(config-ac)# ap-serial test-serial AP220-SE AP220-SH AP220-E hw-ver 1.0
AC-FS(config-ac)# active-bin-file ap.bin
AC-FS(config-ac)# ap-iamge test-serial ap.bin
```

2. The following exmaple removes the configuration from the AC to make the APs in the product series named test-serial no longer use the ap.bin file for upgrade.

```
AC-FS(config-ac)# no ap-image test-serial ap.bin
```

【Prompt Information】-

【Common Mistake】 --

【Platform Description】-

4.11 ap-subif

Use this command to enable the AP to create the sub interface of the WAN port. Use the no form of this command to remove the configuration.

ap-subif enable no ap-subif enable

【Parameter Description】-

【Default Configuration】-

【Command Mode】AP configuration mode/all AP configuration mode

【Default Level】15

【Usage Guide】 When the AP obtains the address through PPPoE dial-up, the sub-interface of the WAN port of the AP will be automatically deleted. This command will not be able to set the AP to create the sub-interface of the WAN port in dial-up mode.

【Configuration Example】1: Configure AP1 to remove the sub-interface of the WAN port.

```
AC-FS(config)# ap-config AP1
AC-FS(config-ap)# no ap-subif enable
```

【Verification】1: Use the show ap-config running command to check whether the configuration is successful.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.12 ap-vlan

Configure the native VLAN of the AP, and the AP will transmit the frames under this VLAN in the form of UNTAG.

ap-vlan vlan-id

Restore Defaults.

no ap-vlan

【Parameter Description】

Parameter	Description
vlan-id	Configure the VLAN used by the wired network interface. vlan-id: The specified VLAN, the value range is 1~4094, the default value is 1.

【Usage Guide】 The AP untags the frame of the Native VLAN before forwarding it. In local forwarding mode, if the user VLAN is the same as the Native VLAN, the frame is forwarded untagged and the access switch determines the VLAN where the user resides.

This command forces the online AP to go offline and enables reconnection.

In WDS deployment, when ROOT-BRIDGE and NONROOT-BRIDGE devices are configured with local forwarding, they should reside in the same AP-VLAN. Otherwise, the NONROOT-BRIDGE device cannot

share the address pool with the ROOT-BRIDGE device; packet forwarding on the NONROOT-BRIDGE device may even be affected.

This command is configured only when the STA of a WLAN wants to access the VLAN where the switch resides while another WLAN requires that its STA resides in VLAN 1, which is not the Native VLAN.

If the static DHCP address pool is configured, and BVI 1 port number is used as client ID, this configuration will bring changes to the BVI port. In this case, the DHCP server configuration should be modified. Otherwise, the address cannot be obtained.

When the AP obtains the address through PPPoE and CAPWAP selects dialer 1 as the source port, the STA traffic is forwarded

untagged even if this command is configured.

【Configuration Examples】 The following example sets the Native VLAN for AP 1 to 20. The following example sets the Native VLAN for AP 1 to 20.

```
AC-FS(config)# ap-config AP1
AC-FS(config-ap)# ap-vlan 20
```

【Verification】1: Use the show ap-config running command to check whether the configuration is successful.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.13 ap-upgrade bandwidth

Use this command to configure the upgrade bandwidth for AP devices. Use the no form of this command to restore the default setting.

ap-upgrade band-widthnum

no ap-upgrade band-width

【Parameter Description】

Parameter	Description
num	Bandwidth for AP upgrade, namely, the push rate for the AP upgrade file. The range is from 1 to 1,024. The unit is 1 KB. The default value is 0.

【Default Configuration】 No bandwidth limit.

【Command Mode】 AP configuration mode

【Default Level】15

【Usage Guide】 1. The configuration only limits the bandwidth control of AP centralized upgrade from AC. Distributed upgrade is not directly affected by this configuration, but the distributed upgrade data source is the root AP through centralized upgrade, so distributed

upgrade is indirectly affected by this configuration.

2. The unit is 1KB. For example, if the minimum available bandwidth on the link between AP and AC is 1Mbps, configure 128.

【Configuration Example】 1: Configure the upgrade bandwidth for the AP, of which 128 is converted into a bandwidth of 1Mbps, that is, the maximum bandwidth occupied by the AP centralized upgrade is 1M.

```
AC-FS(config-ac)# ap-upgrade band-width 128
```

【Verification】 1: Use the show ap-config running-config command to check whether the configuration is successful.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

4.14 ap-upgrade group

Configure the AP to join the upgrade group.

ap-upgrade group group-name

Unconfigure.

no ap-upgrade group

【Parameter Description】

Parameter	Description
group-name	Upgrade group name.

【Default Configuration】 -

【Command Mode】 AP configuration mode

【Usage Guide】 The following configuration restrictions are applied on the AP devices which are added to a upgrade group:

1. The AP devices in the same group need to be configured with the ap-grade band-width command, so that the upgrade bandwidth of the AP devices is identical.

2. The capwap upgrade group command should be configured before this command.

3. When no configuration, if there is an ap in the group, it is not allowed to delete the group

【Configuration Examples】 The following example adds an AP device to the upgrade group UPGRADE-GROUP1.

```
AC-FS(config-ac)# ap-upgrade group UPGRADE-GROUP1.
```

【**Verification**】1: Use the show ap-config running-config command to check whether the configuration is successful.

【**Prompt Information**】-

【**Common Mistake**】-

【**Platform Description**】-

4.15 capwap ctrl-ip

Use this command to set the IPv4 address for the CAPWAP tunnel between the AC and the AP. Use the no form of this command to restore the default setting.

capwap ctrl-ip ip-address

Unconfigure.

no capwap ctrl-ip

【**Parameter Description**】

Parameter	Description
ip-address	Specifies the IP address for the CAPWAP tunnel between the AC a should be an interface IP address of the AC.

【**Default Configuration**】 -

【**Command Mode**】 AP configuration mode

【**Usage Guide**】 The AC generally uses a Loopback address to create the CAPWAP tunnel. This command enables the AC to create the CAPWAP tunnel with interface addresses in other three layers.

1. The configuration may disconnect the AP that is already online.

2. Configuring an address that does not exist on the AC will prevent the CAPWAP tunnel from being established

3. When the gateway of the AP is not in the AC (that is, the AC and AP are in a Layer 3 topology), the option option of the address pool of the AP should be configured with the address configured by capwap ctrl-ip (if configured).

【Configuration Examples】 The following example sets the IP address for the CAPWAP tunnel between the AC and the AP to 10.0.0.1.

```
AC-FS(config-ac)# capwap ctrl-ip 10.0.0.1
```

【Verification】1: Use the show ap-config running-config command to check whether the configuration is successful.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.16 capwap discovery-type ac-referral

Configure the AC to allow AP discovery through referral type discovery packets.

capwap discovery-type ac-referral allow

Configuring the AC does not allow APs to be discovered through referral-type discovery packets.

capwap discovery-type ac-referral forbidden

【Parameter Description】

【Default Configuration】 Allow AP to discover AC through referral type discovery packets

【Command Mode】AC configuration mode

【Default Level】15

【Usage Guide】 CAPWAP standard protocol, used for AP to discover whether there is an AC in the environment. If it is not allowed, the AP will use this type of discovery packet, and the AC will not reply to the AP, thus rejecting the AP to establish CAPWAP with the current AC tunnel.

If the configuration is not allowed, all APs will not be able to establish CAPWAP tunnels with this AC in the form of referrals.

【Configuration Example】 1: Configure the AP to not allow discovery of ACs through referral type discovery packets

```
AC-FS(config-ac)# capwap discovery-type ac-referral forbidden
```

【Verification】 1: Use the show running-config command to check whether the configuration is successful.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 Only AC supports this command

4.17 capwap discovery-type all

Configuring the AC allows APs to be discovered by how to discover types.

capwap discovery-type all allow

Configuring the AC does not allow APs to be discovered in the form of how to auto-discover.

capwap discovery-type all forbidden

【Parameter Description】-

【Default Configuration】Allow AP to discover AC through how to automatically discover。

【Command Mode】AC configuration mode

【Default Level】15

【Usage Guide】 CAPWAP standard protocol, used by AP to discover whether there is an AC in the environment. The current discovery forms are (referral, DHCP, DNS, static configuration, and others). If the configuration is not allowed, the discovery packet sent by the AP , the AC side does not reply, thus rejecting the AP to establish a CAPWAP tunnel with the current AC.

If the configuration is not allowed, all APs cannot establish CAPWAP tunnels with this AC through discovery packets.

【Configuration Example】 1: Configure the AP to not allow the AC to be discovered by how to automatically discover it

```
AC-FS(config-ac)# capwap discovery-type all forbidden
```

【Verification】 1: Use the show running-config command to check whether the configuration is successful.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 Only AC supports this command

4.18 capwap discovery-type dhcp

Configure the AC to allow AP discovery through DHCP-type discovery packets.

capwap discovery-type dhcp allow

Configuring the AC does not allow APs to be discovered through DHCP-type discovery packets.

capwap discovery-type dhcp forbidden

【Parameter Description】-

【Default Configuration】Allow the AP to discover the AC through DHCP-type discovery packets

【Command Mode】AC configuration mode

【Default Level】15

【Usage Guide】 CAPWAP standard protocol, used for AP to discover whether there is an AC in the environment. If it is configured to not allow DHCP discovery, the AP uses this type of

The AC does not reply to the discovery packet, thus rejecting the AP to establish a CAPWAP tunnel with the current AC.

If the configuration is not allowed, the AC address obtained by the AP through DHCP cannot establish a CAPWAP tunnel with this AC.

【Configuration Example】1: Configure the AP to not allow DHCP type discovery packets to discover the AC

```
AC-FS(config-ac)# capwap discovery-type dhcp forbidden
```

【Verification】 1: Use the show running-config command to check whether the configuration is successful.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 Only AC supports this command

4.19 capwap discovery-type dns

Configure the AC to allow APs to be discovered through DNS-type discovery packets.

capwap discovery-type dns allow

Configuring the AC does not allow APs to be discovered through DNS-type discovery packets.

capwap discovery-type dns forbidden

【Parameter Description】-

【Default Configuration】Allow the AP to discover the AC through DNS-type discovery packets.

【Command Mode】AC configuration mode

【Default Level】15

【Usage Guide】 If the configuration is not allowed, the AC address obtained by the AP through DNS will not be able to establish a CAPWAP tunnel with this AC.

If the configuration is not allowed, the AC address obtained by the AP through DNS will not be able to establish a CAPWAP tunnel with this AC.

【Configuration Example】1: Configure the AP to not allow DNS type discovery packets to discover the AC

```
AC-FS(config-ac)# capwap discovery-type dns forbidden
```

【Verification】1: Use the show running-config command to check whether the configuration is successful.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 Only AC supports this command

4.20 capwap discovery-type static-config

Configuring an AC allows APs to be discovered through discovery packets of the statically configured AC address type.

capwap discovery-type static-config allow

Configuring an AC does not allow APs to be discovered through discovery packets of the statically configured AC address type.

capwap discovery-type static-config forbidden

【Parameter Description】-

【Default Configuration】 Allow AP to discover through statically configured AC address type discovery packets

【Command Mode】AC configuration mode

【Default Level】15

【Usage Guide】CAPWAP standard protocol, used by AP to discover whether there is an AC in the environment. The statically configured AC address has acip. If a statically configured AC address is not allowed to be discovered, the AP will use this type of discovery packet, and the AC will not reply, thus rejecting the AP to establish a CAPWAP tunnel with the current AC.

If the configuration is not allowed, the AP will be unable to establish a CAPWAP tunnel with the AC through the statically configured AC address.

【Configuration Example】1: Configure the AP to not allow discovery packets of the statically configured AC address type to discover the AC.

AC-FS(config-ac)# capwap discovery-type static-config forbidden

【Verification】1: Use the show running-config command to check whether the configuration is successful.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 Only AC supports this command

4.21 capwap discovery-type unknown

Configuring the AC allows APs to be discovered through other types of discovery packets.

capwap discovery-type unknown allow

Configuring the AC does not allow APs to be discovered through other types of discovery packets.

capwap discovery-type unknown forbidden

【Parameter Description】-

【Default Configuration】 Allow AP to discover AC through other types of discovery packets

【Command Mode】AC configuration mode

【Default Level】15

【Usage Guide】 CAPWAP standard protocol, used by AP to discover whether there is an AC in the environment. Other types are types other than referral, DHCP, DNS, and static configuration, such as broadcast and multicast. If this type of discovery is not allowed, the AP will use this type of discovery packet, and the AC will not reply, thus rejecting it. This AP establishes a CAPWAP tunnel with the current AC.

If the configuration is not allowed, the AP will not be able to establish a CAPWAP tunnel with this AC through other types of discovery packets.

【Configuration Example】1: Configure the AP to not allow other types of discovery packets to discover the AC

```
AC-FS(config-ac)# capwap discovery-type unknown forbidden
```

【Verification】1: Use the show running-config command to check whether the configuration is successful.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 Only AC supports this command

4.22 capwap disc-concurrent

Configure the AP's ability to process capwap discovery packets, in PPS.

capwap disc-concurrent num

【Parameter Description】

Parameter	Description
num	The number of discovery packets processed per second, which varies according to product capabilities

【Default Configuration】 The default is different according to the AC capability value.

【Command Mode】AC configuration mode

【Default Level】15

【Usage Guide】 In the market, it is found that APs are madly discovering packets. The CAPWAP module should control the concurrency of discovery packets according to the AC capability. After this command is configured, when the number of packets per second exceeds the configured value, the This discovery packet is discarded and no longer processed.

【Configuration Example】1: Configure the number of AC discovery packets processed。

```
AC-FS(config-ac)# capwap disc-concurrent 512
```

【Verification】1: Use the show capwap server state command to view the configured concurrency value.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 Only AC supports this command

4.23 Capwap DTLS Enable

Configure CAPWAP control channel dtls encryption.

capwap dtls enable

Configure the CAPWAP control channel without encryption.

no capwap dtls enable

【Parameter Description】

【Default Configuration】 The dtls encryption function of CAPWAP control channel is enabled by default.

【Command Mode】AC configuration mode

【Default Level】15

【Usage Guide】 By default, the dtls encryption function of the control channel of CAPWAP is enabled, which can ensure the security of the control interaction between the AC and the AP. In special cases, for the convenience of testing, the user can configure the control channel not to be encrypted.

【Configuration Examples】The following example enables DTLS encryption for the CAPWAP tunnel.

```
FS(config)# ac-controller
FS(config-ac)# capwap dtls enable
```

【Verification】1: Use the show running-config command to check whether the configuration is successful.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

4.24 capwap fragment enable

Enable CAPWAP fragmentation.

capwap fragment enable

Disable CAPWAP fragmentation.

no capwap fragment enable

【Parameter Description】-

【Default Configuration】 By default, the CAPWAP fragmentation function is not enabled.

【Command Mode】 AP configuration mode or AP group configuration mode.

【Default Level】15

【Usage Guide】 After the data packet is encapsulated by the CAPWAP tunnel, the packet length may exceed ip mtu, and the packet will be fragmented by IP. When the ip mtu of multiple nodes in the link are inconsistent, the packet may need to be fragmented and reassembled multiple times, which reduces the packet forwarding performance. The CAPWAP fragmentation function can be enabled

through this command, and the packet will be fragmented during CAPWAP encapsulation. The length of the CAPWAP fragmented packet can be specified by the capwap mtu command as the minimum mtu in the link to avoid IP fragmentation.

【Configuration Example】 1: Enable the CAPWAP fragmentation function of configuring AP1

```
AC-FS(config)# ap-config AP1
AC-FS(config-ap)# capwap fragment enable
```

【Verification】 1: Use the show ap-config running command to check whether the configuration is successful.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

4.25 capwap max-concurrent

Configure the maximum number of concurrent APs allowed by the AC.

capwap max-concurrent num

Unconfigure.

no capwap max-concurrent

【Parameter Description】

Parameter	Description
num	The maximum number of concurrent online APs, in the range from 1 to 200.

【Default Configuration】 The default is 50.

【Command Mode】 AC configuration mode.

【Default Level】 15

【Usage Guide】 If too many APs go online concurrently, AC CPU may increase even to 100%. This will cause the tunnel disconnection. Therefore, it is necessary to limit the number of concurrent online APs.

If you set a small value, the total online time of all APs associated to the AC will be long.

【Configuration Examples】 The following example sets the maximum number of concurrent online APs to 100.

```
AC-FS(config-ac)#capwap max-concurrent 100
```

【Verification】1: Use the show ap-config running command to check whether the configuration is successful.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.26 capwap max-retransmit

Configure the maximum number of retransmissions of CAPWAP packets.

capwap max-retransmit num

Unconfigure.

no capwap max-retransmit

【Parameter Description】

Parameter	Description
num	The maximum number of retransmissions, the default value is 5, the range is 3~60

【Default Configuration】 The default is 5.

【Command Mode】 AP configuration mode/AP group configuration mode

【Default Level】 15

【Usage Guide】 If the CAPWAP request packet is not responded, the packet is retransmitted, The retransmission interval increases by the initial retransmission interval (the smaller value between three seconds and half echo-interval) and the maximum retransmission interval should be no greater than the smaller value between half echo-interval and 60 seconds. If the device does not receive the

response packet within the maximum count, the tunnel is considered disconnected. This command is only effective when the tunnel is in the Run state.

【Configuration Examples】 The following example sets the maximum retransmission count to 20.

```
FS(config)# ap-config AP1
FS(config-ap)#capwap max-retransmit 20
```

【Verification】1: Use the show ap-config running command to check whether the configuration is successful.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.27 capwap upgrade group

Use this command to configure an AP upgrade group. Use the no form of this command to remove an AP upgrade group.

capwap upgrade group group-name[max-concurrent num]

no capwap upgrade group [group-namemax-concurrent]

【Parameter Description】

Parameter	Description
group-name	Upgrade group name.
num	The upgrade group allows the number of concurrent centralized upgrade APs, the default is 5, the range is 1~200.

【Default Configuration】 -

【Command Mode】 AC configuration mode

【Default Level】15

【Usage Guide】 Configure an AP upgrade group. The centralized upgrade of bandwidth control takes the upgrade group as the

scheduling unit, and the concurrent number of AC centralized upgrade is evenly distributed to all upgrade groups.

1. By default, the maximum number of concurrency in each upgrade group is 5, which should be the ratio of the maximum available bandwidth of the group to the maximum available bandwidth of each ap.

【Configuration Examples】 The following example creates an AP upgrade group Upgrade-Group1 and sets the concurrent number to 10.

```
AC-FS(config-ac)# capwap upgrade group Upgrade-Group1 max-current 10
```

【Verification】 1: Use the show ap-config running command to check whether the configuration is successful.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

4.28 capwap mtu

Configure the path mtu for the CAPWAP tunnel.

capwap mtu num

restore default.

no capwap mtu

【Parameter Description】

Parameter	Description
num	CAPWAP path mtu size, Parameter range 68~1500, in bytes

【Default Configuration】 Default mtu size is 1500 bytes.

【Command Mode】 AP configuration mode/AP group configuration mode

【Default Level】 15

【Usage Guide】 When the length of the data packet encapsulated by the CAPWAP tunnel exceeds the path MTU of the CAPWAP tunnel, CAPWAP will fragment the data packet. When configuring the tunnel path MTU, please set it to the minimum IP MTU on the tunnel path, so as to avoid IP fragmentation and reassembly during packet forwarding and reduce the forwarding performance.

If the MTU is set too small, a large number of fragmented packets will be generated, which will affect the packet forwarding performance, and even cause large packets to fail to be transmitted. Therefore, please plan the MTU size reasonably.

【Configuration Examples】 The following example sets the PMTU for the CAPWAP tunnel to 1200 bytes.

```
AC-FS(config)# ap-config AP1
AC-FS(config-ap)# capwap mtu 1200
```

【Verification】1: Use the show ap-config running command to check whether the configuration is successful.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.29 capwap upgrade max-concurrent

Configure the maximum number of concurrent AP upgrades allowed by the AC.

capwap upgrade max-concurrent num

unconfigure.

no capwap upgrade max-concurrent

【Parameter Description】

Parameter	Description
num	The maximum number of concurrent AP upgrades, the range is 1~200.

【Default Configuration】The default maximum number of APs going online concurrently is 15.

【Command Mode】AC configuration mode.

【Default Level】15

【Usage Guide】 If too many APs upgrade concurrently, AC CPU may increase even to 100%. This will cause tunnel disconnection. Therefore, it is necessary to limit the number of concurrently upgrading APs.

【Configuration Examples】 The following example sets the maximum number of concurrently upgrading APs to 10.

```
AC-FS(config-ac)#capwap upgrade max-concurrent 10
```

【Verification】1: Use the show ap-config running command to check whether the configuration is successful.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.30 echo-interval

Configure the heartbeat keepalive interval for CAPWAP.

echo-interval seconds

Restore default

no echo-interval

【Parameter Description】

Parameter	Description
seconds	CAPWAP heartbeat keep-alive interval, the range is 5~255, the unit is seconds.

【Default Configuration】 The default value of the keepalive interval is 30s.

【Command Mode】 AP configuration mode or AP group configuration mode

【Default Level】15

【Usage Guide】 In the thin AP network architecture, the AC and AP are interconnected through CAPWAP tunnels. Echo Request and Echo Response are used between AP and AC to maintain link validity. When there are no other request packets, the AP sends Echo Request packets every echo-interval to keep alive. If the AP does not receive a response packet, the packet will be retransmitted. The retransmission is doubled at the initial retransmission interval (the minimum value of 3 seconds and half of the echo-interval), and the

maximum retransmission interval cannot exceed the echo interval. Half of -interval with a minimum of 60 seconds. When the maximum number of retransmissions is still not received, the tunnel is considered disconnected. That is, the keep-alive failure time of the tunnel is the keep-alive time plus the retransmission interval. This command takes effect only when the tunnel is in Run state. The default echo-interval is 30s, and the default maximum number of retransmissions is 5. After the request message is sent at 0s, if no response is received, the retransmission message is retransmitted at intervals of 3s, 6s, 12s, 15s, and 15s respectively. Configure echo-interval and max-retransmit to other values and still calculate the packet timeout according to this rule.

When deploying a wireless network, you can adjust the echo-interval according to the network scale to plan the network convergence performance. When adjusting, make sure that you have a sufficient understanding of the network scale and that the convergence is really needed. Avoid setting too low a value in the wireless network of large-scale AP deployment. impact on the network environment.

【Configuration Examples】 The following exmaple configures a 10-second echo interval for AP0001.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# echo-interval 10
```

The following example configures a 10-second echo interval for all APs.

```
AC-FS(config)# ap-config all
AC-FS(config-ap)# echo-interval 10
```

The following example configures a 10-second echo interval for all APs in the default AP group.

```
AC-FS(config)# ap-group default
AC-FS(config-ap-group)# echo-interval 10
```

【Verification】 1: Use the show ap-config running command to check whether the configuration is successful.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

4.31 exec-CMD

Configure an AP to execute a command.

exec-cmd mode exec-mode cmd exec-cmd [slot id | all] once

Configuring APs in an AP Group to Execute a Command.

exec-cmd exec-cmd

Unconfigure.

no exec-cmd mode exec-mode cmd exec-cmd [slot id | all]

【Parameter Description】

Parameter	Description
exec-mode	The mode in which the command is executed on the AP.
exec-cmd	Commands executed on AP or corresponding ap-config.
id	Smart points + the slot number of the map connected to the host.
all	Zhifen + all maps under the host.
once	The command is executed only once, without saving.

【Default Configuration】 -

【Command Mode】 AP configuration mode/all AP configuration mode or AP group configuration mode.

【Default Level】 15

【Usage Guide】 Some configuration commands are currently only supported on the AP, and there is no corresponding configuration command on the AC. If you want to perform such configuration on the AP on the AC, you can use the exec-cmd command under ap-config to implement. It should be noted that if you need to cancel or change the configuration in exec-cmd, you need to use the no exec-cmd command to delete the corresponding configuration, and then use the exec-cmd command to reverse or change the configuration; extend exec-cmd It can send the corresponding command to the MAP through the AC, and execute the command on the MAP, and the rest is no different from the ordinary ap;

If you configure ap-config all and a separate ap-config at the same time, for online APs, the later configuration will take effect. For offline configuration, if the AP is online, it will take effect according to the priority ap-config > ap-config all;

Some configuration commands are only supported in ap-config mode, but there are no corresponding configuration commands in ap-group. If you need to configure such commands on all APs in an AP group, you can execute the exec-cmd command in the AP group. It should be noted that this configuration is not saved in ap-group mode, but is equivalent to executing this command once for all APs in the current AP group.

【Configuration Example】1: Disabling the EWEB function of the AP on the AC.

```
AC-FS(config)#ap-config AP1
AC-FS(config-ap)# exec-cmd mode configure cmd "no enable service web-server all"
```

2: Configure the EWEB function of the AP to restart on the AC/

```
AC-FS(config-ap)# no exec-cmd mode configure cmd "no enable service web-server all"
AC-FS(config-ap)# exec-cmd mode configure cmd "enable service web-server all"
```

3: Configure all APs in the AP group to disable the AP's EWEB function/

```
AC-FS(config-group)#exec-cmd exec-cmd mode configure cmd "no enable service web-server all"
```

【Verification】1: Use the show ap-config running command to check whether the configuration is successful.

【Prompt Information】-

【Common Mistake】 Change the configuration of exec-cmd, if there is no configuration no exec-cmd delete the original configuration, or do not re-configure the reverse configuration through exec-cmd

【Platform Description】-

4.32 install update

Update the micro AP installation status of Zhifen+AP.

install update

【Parameter Description】-

【Default Configuration】-

【Command Mode】 AP configuration mode

【Default Level】15

【Usage Guide】A micro AP has been installed in the designated slot of Zhifen+AP. If the micro AP is manually removed later, the system will consider the micro AP offline. This command will query the currently online Zhifen+AP, and use its online micro AP as the installed

micro AP. This command does not save the configuration.

【Configuration Example】1: Update the installation status of all micro APs.

```
AC-FS(config)# ap-config all
AC-FS(config-ap)# install update
```

【Verification】1: Use the show ap-config slot command to view the new micro AP installation information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.33 ip address

Configure the static IP address of the specified AP.

ip address ip-address network-mask gateway

Revert to Default Configuration.

no ip address

【Parameter Description】

Parameter	Description
ip-address	Interface address of the AP.
network-mask	Address mask of the AP.
gateway	Gateway of the AP.

【Default Configuration】 -

【Command Mode】 AP configuration mode

【Default Level】15

【Usage Guide】 The AP can obtain its own IP address through static configuration and DHCP. If the AP has not been configured with a static IP address, it can dynamically obtain the address by DHCP and join the AC. At this time, you can configure the static address of the AP through this command, so that the address will remain unchanged after the AP is restarted.

1. Setting the AP's address as a static address will disable the DHCP function. At this time, the AC address cannot be obtained through the DHCP OPTION option. Therefore, before configuring this command, you need to configure the connected AC through the "acip" command in the AP configuration mode. address so that the AP and AC can discover and join the AC when they are not on the same subnet.

2. If the current address of the AP is inconsistent with the address specified by this command, the static address of the AP will be updated and the CAPWAP tunnel will be rebuilt.

【Configuration Examples】 The following example configures the address of AP0001 as 1.1.1.1, its mask as 255.255.255.0, and its next hop as 1.1.1.2.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# ip address 1.1.1.1 255.255.255.0 1.1.1.2
```

【Verification】 1: Use the show ap-config running command to check whether the configuration is successful.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

4.34 link-latency

Configure to detect the link status between the AC and the APs in the specified AP group.

link-latency

Unconfigure.

no link-latency

【Parameter Description】 -

【Default Configuration】 -

【Command Mode】 AP configuration mode/AP group configuration mode

【Default Level】 15

【Usage Guide】-

【Configuration Example】1: Enable to detect the link status between the specified AP-0001 and AC, and check the corresponding link status information.

```
AC-FS(config)# ap-config AP-0001
AC-FS(config-ap)# link-latency
```

2: Enable the AP group "default" to detect the link status between AC and AP, and check the link status information of the specified AP-0001.

```
AC-FS(config)# ap-group default
AC-FS(config-ap-group)# link-latency
```

【Verification】1: Use the show ap-config link-latency command to view the link status information between the AC and the AP.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.35 location

Configure the location information of the AC or AP.

location location-string

Revert to Default Configuration.

no location

【Parameter Description】

Parameter	Description

location-string	Indicates AC location information, which can consist of up to 255 characters without any space.

【Default Configuration】 By default, the AC location information is FS_COM, the AP location information is null.

【Command Mode】 AC configuration mode/AP configuration mode

【Default Level】 15

【Usage Guide】 None

【Configuration Example】1: The location for configuring a specific AC is the second floor of the computer system (computer-layer2)

```
AC-FS(config-ac)# location computer-layer2
```

2: Configure the location information of AP0001 as AP-company.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# location AP-company
```

【Verification】1: Use the show ac-config running command to view the AC location information.

2: Use the show ap-config running command to view the AP location information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.36 pass-vlan

In smart division + AP cascading or ring networking, configure the transmission vlan of the AP host, so that when users of different AP hosts plan different vlans, user packets can be forwarded through the uplink AP host.

pass-vlan vlan-range

Restore Defaults。

no pass-vlan vlan-range

【Parameter Description】

Parameter	Description
vlan-range	A list of VLAN ID ranges, you can specify multiple VLAN IDs, separated by commas or dashes. A comma separates two VLAN IDs, and a horizontal bar represents two VLAN ID ranges.

【Default Configuration】 The default is not configured.

【Command Mode】 AP configuration mode

【Default Level】15

【Usage Guide】 1. This command can be configured for all APs, but the configuration is only valid for the Smart+AP host.

2. This configuration will create the corresponding vlan on the host of Zhifen+AP, so that the host can forward the packets of the corresponding vlan. At the same time, the pass-vlan will be automatically trimmed on the downlink port of the host to prevent the broadcast and multicast packets of other hosts from flooding to the downlink AP of the host.

The vlan specified by this configuration cannot conflict with the vlan specified by the interface-mapping, ap-vlan, and wired-vlan commands, nor can the vlan 2444 for the internal management of Zhifen+AP be configured.

【Configuration Example】1: Configure the transport VLAN of AP1 to use VLAN 20。

```
AC-FS(config)# ap-config AP1
AC-FS(config-ap)# pass-vlan 20
```

【Verification】1: Use the show ap-config running command to check whether the configuration is successful.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.37 reset slot

Restart the micro AP of Zhifen+AP.

reset slot slot-id

【Parameter Description】

Parameter	Description
slot-id	Slot number, range 1~24.

【Default Configuration】-

【Command Mode】 AP configuration mode.

【Default Level】15

【Usage Guide】 This command is only valid for Zhifen + AP devices, and does not support configuring all APs. The configuration is not saved.

The slot targeted by this command is the slot number of the host. In the cascading scenario, it will take effect on the two micro APs under the slot number at the same time.

【Configuration Example】1: Restart the micro AP1 of AP0001.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# reset slot 1
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.38 set version

Use this command to set the version number.

set-version string

【Parameter Description】

Parameter	Description
string	Sets the version number.

【Default Configuration】-

【Command Mode】 AC configuration mode

【Default Level】15

【Usage Guide】 This command is used to set the version number and push version number to APs.

【Configuration Examples】 The following example sets the version number to FSOS 10.4(2B17)-SP2.

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# set-version FSOS 10.4(2B17)-SP2
```

【Verification】Use the show version command to check the version.

【Prompt Information】-

【Platform Description】 -

4.39 show ac-config active-file

Displays a list of files that have been activated in this AC.

show ac-config active-file

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】15

【Usage Guide】 -

【Configuration Examples】 The following example displays a list of activated files on the current AC.

```
AC-FS#show ac-config active-file
Cnt    File Name                          Image Id            Software number      Type
Used Cnt  DL Cnt Ready

1      ap220ev1.1-mid(6-3).bin            RGOS 10.X-UPG       NA                   rgos10     0
0          Init
2      ap220.bin.....1.0.0.017ed304       M09092708272014     main
0          0          Init
```

Field	Description
Cnt	Active file list number
File Name	active filename
Image Id	Active file version
Software number	Active file compilation date
Used Cnt	Indicates how many APs are currently using this file
DL Cnt	Indicates how many APs the upgrade file has been downloaded to
Ready	Indicates whether the file has been fully activated.

【Prompt Information】-

【Platform Description】 -

4.40 show av-vonfig serial-product

Use this command to display the correspondence association between the AP product series and product models configured of the AC, and display which files should be used to upgrade the corresponding product series.

show ac-config serial-product

【Parameter Description】 -

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 15

【Usage Guide】 -

【Configuration Examples】 The following example displays the AP product series and product models configured for the current AC.

```
AC-FS#show ac-config serial-product

Cnt      Serial Name      Hardware Version File Name      AP Product ID
-------------------------------------------------------------
1        ap-ser1.x        1.x              ap220-1.bin AP220-E
                                                         AP220-SE
                                                         AP220-SH
                                                         AP620-H

                                                         AP220-E(M)
2        ap-ser2.x        2.x              ap220.bin     AP220-E

                                                         AP220-E(M)
```

Field	Description
Cnt	display number
Serial Name	AP product family
Hardware Version	Hardware version number
File Name	Upgrade files corresponding to AP product series
AP Product ID	AP product model

【Prompt Information】-

【Platform Description】-

4.41 show ac-config upgrade-group

Use this command to display the upgrade groups and AP devices on the AC device.

show ac-config upgrade-group [group-name]

【Parameter Description】

Parameter	Description
group-name	AP upgrade group name.

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 15

【Usage Guide】 -

【Configuration Examples】 1. The following example displays AP upgrade groups.

```
AC-FS#show ac-config upgrade-group
Cnt    Group-Name                Max-Concurrent    Token cnt    Upgrading cnt
-----  ------------------------------------------  -----------  -------------

1      UPGRADE-GROUP1              10               2            1
```

Field	Description
Cnt	display number
Group-Name	AP upgrade group name
Max-Concurrent	The maximum number of concurrent upgrades in this group
Token cnt	The number of upgrades currently allocated
Upgrading cnt	Number of APs being upgraded

2: Display the AP information in the upgrade group.

```
AC-FS#show ac-config upgrade-group UPGRADE-GROUP1
Group have 2 ap,  online 1 offline 1
Cnt     Ap-Name                   Ap-Mac              Online    Upgrade      Band-width
------  ------------------------  ------------------  --------  -----------  ----------

1       ap220e                    8832.0000.1111      true       true         128
2       ap330-------------------------------------- false      false        128
```

Field	Description
Cnt	display number.
Ap-Name	AP name.
Ap-Mac	AP's MAC address.
Online	is online.
Upgrade	Is it being upgraded.
Band-width	Bandwidth configuration for this AP.

【Prompt Information】-

【Platform Description】-

4.42 show ap-config board-data

Use this command to display the board data information of an AP.

show ap-config board-dataap-name

【Parameter Description】

Parameter	Description
ap-name	Indicates the name of the AP to be queried.

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 15

【Usage Guide】-

【Configuration Examples】 The following example displays the board data information of an AP.

```
ac#show ap-config board-data wlan-ap-0001 Ap(wlan-ap-0001)'s board data:
wtp model num   :
wtp serial num    1234567890123
board id     : AP220E
```

Field	Description
wtp model num	Product number.
wtp serial num	AP serial number.
board id	motherboard id.
board reversion	motherboard version.
base address	system mac.

【Prompt Information】 -

【Platform Description】 -

4.43 show ap-config inventory

Use this command to display the manufacturer information about an AP.

show ap-config inventoryap-name

【Parameter Description】

Parameter	Description
ap-name	Indicates the name of the AP to be queried.

【Default Configuration】 -

【Command Mode】 Privileged mode

【Default Level】 15

【Usage Guide】 -

【Configuration Examples】 The following example displays the manufacturer information of an AP.

```
ac#show ap-config inventory wlan-ap-0001 AP Name:  wlan-ap-0001
Location:
Product Id:  AP220E Vendor Id:  31762
SN:  1531991320
```

Field	Description
AP Name	AP name.

Location	AP location.
Product Id	product id.
Vendo Id	manufacturer id.
SN	serial number.

【Prompt Information】-

【Platform Description】 -

4.44 show ap-config link-latency

Use this command to check the link status between AC and AP.

show ap-config link-latency {all | singleap-name}

【Parameter Description】

Parameter	Description
all	Query all APs.
single	Query a single AP.
ap-name	The name of the AP to query.

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 15

【Usage Guide】 -

【Configuration Examples】 1: View the link status between a single AP and AC.

```
ac#show ap-config link-latency single ap330
AP Name                                  Status      Current    Maximum   Minimum   Number
-------------------------------------------------------------------------------------------
ap330                                    Disabled    0ms        0ms       0ms       0
```

Field	Description
AP Name	AP name.
Status	link status.
Current	current link delay.
Maximum	maximum link delay.
Minimum	Minimum link delay.
Number	Maximum link delay, number of uploads.

【Prompt Information】-

【Platform Description】-

4.45 show ap-config reboot

Use this command to display the reboot information about an AP.

show ap-config reboot ap-name

【Parameter Description】

Parameter	Description
ap-name	Indicates the name of the AP to be queried.

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 15

【Usage Guide】 -

【Configuration Examples】 1: Query AP restart statistics.

```
AC-FS#show ap-config reboot ap330
Ap(ap330)'s  reboot  statistic:
Reboot Cnt          :67
AC Init Cnt           :0
Link Fail Cnt         :0
SW Fail Cnt           :0
HW Fail Cnt           :0
Other Fail Cnt      :67
Unknow Fail Cnt     :0
Last Fail Type          :0
```

Field	Description
Reboot Cnt	Number of restarts.
AC Init Cnt	AC initialization times.
Link Fail Cnt	Number of link failures.
SW Fail Cnt	Software failures.
HW Fail Cnt	hardware failures.
Other Fail Cnt	Failures for other reasons.
Unknow Fail Cnt	Unknown reason failures.
Last Fail Type	last failure type.

【Prompt Information】-

【Platform Description】-

4.46 show ap-config slot

Display the micro AP information of the specified AP.

show ap-config slot ap-name

【Parameter Description】

Parameter	Description
ap-name	The name of the AP to query

【Command Mode】 Privileged mode

【Default Level】15

【Usage Guide】 This command only displays the information of the online intelligence + AP device.

【Configuration Example】1: Display the AP's micro AP information.

```
AC-FS#show ap-config slot AM5528(EP)
Radio: Radio ID
       E = enabled, D = disabled, N = Not exist
       Current Sta number
       Channel: * = Global
       Power Level = Percent
```

```
Install Slot Number: 48
Online Slot Number: 11
Offline Slot Number: 37
Slot ID Role    Slot Name                      Model     Slot Mac       Radio
Radio              Up/Off time  State

1       master     19#4F_wenmi                    MAP552.....5869.6c36.e29b 1  E   3    9    50
2  E   6  165   100    0:04:18:03 online
2       master     19#4F_fangjian_1               MAP752(ST)5869.6c36.e22d 3  E   4   13    50
4  E   5  153   100    0:04:17:58 online
2       slave 19#4F_fangjian_2               MAP752(ST)5869.6c36.e32c 5  E   3    6    50 6  E
3   36   100    0:04:17:52 online
```

Field Description:

Field	Description
Install Slot Number	The number of micro APs installed on this AP.
Online Slot Number	The number of micro APs online in this AP.
Offline Slot Number	The number of micro APs that the AP is offline.
Slot ID	The slot number where the micro AP is located.
Role	The cascade relationship of micro APs, the master micro AP is the master, and the slave micro AP is the slave.
Slot Name	Micro AP name.
Model	Micro AP Model.
MAC Address	MAC address of the micro AP.
Radio	Radio ID, status, number of users, channel and power corresponding to

	the micro AP.
Up/Off time	online or offline time.
State	online or offline status.

【Prompt Information】-

【Platform Description】-

4.47 show ap-config static-ip

Displays the location information of all APs.

show ap-config static-ip { all | singleap-name}

【Parameter Description】

Parameter	Description
all	Query all APs.
single	Query a single AP.
ap-name	The name of the AP to query.

【Command Mode】 Privileged mode

【Default Level】15

【Usage Guide】 -

【Configuration Examples】 1: Display the static address of the AP

It contains AP name, AP ip address, mask and gateway.

```
AC-FS#show ap-config static-ip single 0034.5612.78a0
AP Name              Static   IP              Net Mask          Getway
-------------------- -------- --------------- ----------------- ---------------
0034.5612.78a0       Enabled  22.22.22.22     255.255.255.0     22.22.22.53
```

【Prompt Information】-

【Platform Description】 -

4.48 show ap-config summarylocation

Use this command to display location information on all APs.

show ap-config summary location

【Parameter Description】 -

【Default Level】 15

【Command Mode】 Privileged mode

【Usage Guide】 -

【Configuration Examples】 The following example displays location information on all APs, including the AP name, MAC address, location, and status (online/offline).

```
AC-FS#show ap-config summary location
   AP Name
State                                    IP Address          Mac Address       Location
-----------------------------------------------------------------------------------------------------

ap220                                    172.18.100.4        1414.4b13.9ff3    Bangongshi_4#
Run
ap3                                      172.18.100.16       001a.a94e.d40d    building 20#3F
Run
```

【Prompt Information】-

【Platform Description】 -

4.49 show ap-config summary slot

Display the micro AP information of all APs.

show ap-config summary slot

【Parameter Description】 -

【Command Mode】 Privileged mode

【Default Level】15

【Usage Guide】 This command only displays the information of the online intelligence + AP device.

【Configuration Example】1: Display the AP's micro AP information.

```
AC-FS#show ap-config summary slot
Radio: Radio ID
       E = enabled, D = disabled, N = Not exist
       Current Sta number
       Channel: * = Global
       Power Level = Percent

Total AP Number: 1
Total Install Slot Number: 48
Total Online Slot Number: 11
Total Offline Slot Number: 37
```

```
AP(AM5528EP)'s Slots Information
Install Slot Number: 48
Online Slot Number: 11
Offline Slot Number: 37
Slot ID Role    Slot Name                       Model     Slot Mac       Radio
Radio              Up/Off time State

1       master     19#4F_wenmi                    MAP552.....5869.6c36.e29b 1  E   3    9    50
2  E    6  165    100    0:04:18:03 online
2       master     19#4F_fangjian_1               MAP752(ST)5869.6c36.e22d 3  E   4   13    50
4  E    5  153    100    0:04:17:58 online
2       slave 19#4F_fangjian_2                MAP752(ST)5869.6c36.e32c 5  E   3    6    50 6  E
3   36   100    0:04:17:52 online
```

Field Description:

Field	Description
Total Install Number	The number of micro APs installed on all APs.
Total Online Number	Number of micro APs online for all APs.
Total Offline Number	The number of micro APs with all APs offline.
Install Number	The number of micro APs installed in this P.
Online Number	The number of micro APs online in this AP.
Offline Number	The number of micro APs that the AP is offline.

Slot ID	The slot number where the micro AP is located.
Role	The cascade relationship of micro APs, the master micro AP is the master, and the slave micro AP is the slave.
Slot Name	Micro AP name.
Model	Micro AP Model.
MAC Address	MAC address of the micro AP.
Radio	Radio ID, status, number of users, channel and power corresponding to the micro AP.
Up/Off time	online or offline time.
State	online or offline status.

【Prompt Information】-

【Platform Description】-

4.50 show ap-config summary slot interface

Display the downlink interface information of all Zhifen+APs.

show ap-config summary slot interface

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】15

【Usage Guide】-

【Configuration Example】1: Display the information about the downlink interface of Smart Score+AP

```
AC-FS#sh ap-config summary slot interface
AP(00d0.f822.33dc)'s information
AP mac          IP Address      Slot ID Role    Status  Duplex  Speed
--------------- --------------- ------- ------- ------- ------- -------
00d0.f822.33dc 102.102.102.102 1       master  down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 2       master  down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 3       master  down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 4       master  down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 5       master  up      Full    1000M
00d0.f822.33dc 102.102.102.102 6       master  down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 7       master  down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 8       master  down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 9       master  down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 10      master  down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 11      master  down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 12      master  down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 13      master  down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 14      master  down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 15      master  down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 16      master  down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 17      master  down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 18      master  down    Unknown Unknown
00d0.f822.33dc   102.102.102.102   19   master   down   Unknown   Unknown
00d0.f822.33dc   102.102.102.102   20   master   down   Unknown   Unknown
00d0.f822.33dc   102.102.102.102   21   master   down   Unknown   Unknown
00d0.f822.33dc   102.102.102.102   22   master   down   Unknown   Unknown
00d0.f822.33dc 102.102.102.102 23      master  down    Unknown Unknown
00d0.f822.33dc 102.102.102.102 24      master  down    Unknown Unknown
```

Field Description:

Field	Description
AP mac	Smart Score + MAC address of AP host.
IP Address	Smart Score + IP address of the AP host.
Slot ID	Smart Score+AP host downlink interface ID.
Status	Smart Score+AP host downlink interface status.
Duplex	Smart split + AP host downlink interface negotiation duplex status.
Speed	Smart+AP host downlink interface negotiation rate.

【Prompt Information】-

【Platform Description】-

4.51 show ap-config summary group

Displays the intelligence score + AP information in the AP group.

show ap-config summary group

【Parameter Description】

Parameter	Description
apg-name	AP group name

【Command Mode】 Privileged mode

【Default Level】15

【Usage Guide】 None

【Configuration Example】1: Display the intelligence score + AP information in the AP group.

```
AC-FS#sh ap-c summary group group-1
Radio: Radio ID
E = enabled, D = disabled, N = Not exist
Current Sta number
```

```
Channel: * = Global
Power Level = Percent

Total AP Number: 1
Total Install Slot Number: 16
Total Online Slot Number: 1
Total Offline Slot Number: 15

AP(5528ep)'s Slots Information
Install  Slot  Number:  16
Online Slot Number: 1
Offline Slot Number: 15
AP mac Slot ID Role Slot Name Model Slot Mac Radio Radio Up/Off time State

00d0.f822.3434 1 master - MAP752(S) 0000.0006.0000 1 N - - - 2 N---------0:00:08:37 offline
00d0.f822.3434 4 master 00d0.f812.354a MAP752(T) 00d0.f812.354a 7 E 0 11* 100 8 E 0 149* 100 0:00:08:37
online
00d0.f822.3434 5 master - MAP752(T) 00d0.f812.354a 9 N - - - 10 N---------0:00:08:37 offline
00d0.f822.3434 8 master - MAP752(T) 00d0.f812.354a 15 N - - - 16 N---------0:00:08:37 offline
00d0.f822.3434 11 master - MAP752(ST) 00d0.f855.661c 21 N - - - 22 N---------0:00:08:37 offline
00d0.f822.3434 12 master - MAP752(ST) 00d0.f855.661c 23 N - - - 24 N---------0:00:08:37 offline
00d0.f822.3434 13 master - MAP752(ST) 00d0.f855.661c 25 N - - - 26 N---------0:00:08:37 offline
00d0.f822.3434 14 master - MAP752(T) 00d0.f812.354a 27 N - - - 28 N---------0:00:08:37 offline
00d0.f822.3434 15 master - MAP752(T) 00d0.f812.354a 29 N - - - 30 N---------0:00:08:37 offline
00d0.f822.3434 16 master - MAP752(T) 00d0.f812.354a 31 N - - - 32 N---------0:00:08:37 offline
00d0.f822.3434 17 master - MAP752(ST) 00d0.f855.661c 33 N - - - 34 N---------0:00:08:37 offline
00d0.f822.3434 18 master - MAP752(T) 00d0.f812.354a 35 N - - - 36 N---------0:00:08:37 offline
00d0.f822.3434 21 master - MAP752(T) 00d0.f812.354a 41 N - - - 42 N---------0:00:08:37 offline
00d0.f822.3434 22 master - MAP752(ST) 00d0.f855.661c 43 N - - - 44 N---------0:00:08:37 offline
00d0.f822.3434 23 master - MAP752(T) 00d0.f812.354a 45 N - - - 46 N---------0:00:08:37 offline
00d0.f822.3434 24 master - MAP752(T) 00d0.f812.354a 47 N - - - 48 N---------0:00:08:37 offline
```

Field	Description

Total Install Number	The number of micro APs installed on all APs.
Total Online Number	Number of micro APs online for all APs.
Total Offline Number	The number of micro APs with all APs offline.
Install Number	The number of micro APs installed on this AP.
Online Number	The number of micro APs online in this AP.
Offline Number	The number of micro APs that the AP is offline.
Slot ID	The slot number where the micro AP is located.
Role	The cascade relationship of micro APs, the master micro AP is the master, and the slave micro AP is the slave.
Slot Name	Micro AP name.
Model	Micro AP Model.
MAC Address	MAC address of the micro AP.
Radio	Radio ID, status, number of users, channel and power corresponding to the micro AP.
Up/Off time	online or offline time.
State	online or offline status.

【Prompt Information】-

【Platform Description】 Only supported by AC

4.52 show ap-config updating-list

Use this command to display upgrade information on the AP.

show ap-config updating-list

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】15

【Configuration Examples】 The following example displays upgrade information on the AP.

```
AC-FS#show ap-config updating-list
AP NAME                AP PID              File Tx  Time      AP Reset Ready
---------------------- ------------------- -------- --------- --------------

AP220-I                AP220-I             100%     00:00:45  Y
00d0.1414.3f67         AP220-E             98 %     00:00:48  N
```

Field	Description
AP NAME	AP name.
AP PID	AP Product ID.
File Tx	file transfer progress.
Time	Time-consuming to upgrade.
AP Reset Ready	After the upgrade is complete, you can restart.

【Prompt Information】 -

【Platform Description】 -

4.53 show ap-config wtp-descriptor

Use this command to display the status description of an AP.

show ap-config wtp-descriptorap-name

【Parameter Description】

Parameter	Description
ap-name	The name of the AP to query.

【Command Mode】 Privileged mode

【Default Level】 15

【Usage Guide】 -

【Configuration Examples】 1: Display the AP status description.

```
AC-FS#show ap-config wtp-descriptor AP220E-0
Ap(AP220E-0)'s wtp descriptor:
max radio           :2
radio in used       :2

encrypt num         :1
Cnt   WBID    Encry Cap
1  0x1  0xc

sub descriptor num  :3
Cnt      vendor     id    version    type       version    len       version
1    0x7c12    BOOT Ver       21.....1.1.5.0a2945e(140830)
2    0x7c12    ACT SW Ver     14             1.0.0.6b94c319
3    0x7c12    HW Ver         4.....2.00
```

Field	Description
max radio	Maximum number of RF ports.
radio in used	Number of RF ports in use.
encrypt num	Encryption capability supported by wireless port: our company supports ccmp and tkip.

【Prompt Information】 -

【Platform Description】 -

4.54 show ap-config wtp-info

Displays AP status information.

show ap-config wtp-info ap-name

【Parameter Description】

Parameter	Description
ap-name	The name of the AP to query.

【Command Mode】 Privileged mode

【Usage Guide】 N/A

【Default Level】 15

【Configuration Examples】 The following example displays the AP device status.

```
AC-FS#show ap-config wtp-info ap220e
Ap(ap220e)'s status:
AC IP(status):.....101.101.101.101
AP IP(status):      :10.10.10.8 255.255.255.0 10.10.10.2
AP IPV4 ENABLE:     :enable
Location Data:      :
Session ID:         :88320000,111163fb,5c3b3cb3,2cac585a
mac type            :full support
WTP Name:           :ap220e
AP Domain Name:     :ac.AC-FS.com.cn
wired vlan          :0 port  id  1
wired vlan          :0 port  id  2
wired vlan          :0 port  id  3
wired vlan          :0 port id 4
Cw_interface_name   :BVI 1
Cw_wan_interface_ifx::1
Cw_wan_interface_ifx::0
Upgrading State     :Init
AP Image file       :NA
Real version.....1.0.0.641d31e6
Custom version      :AP_RGOS 11.1(2)B1
Upgrade version     :NA
Upgrade from AP     :FALSE
Upgrade for other AP:FALSE
Upgrade from AC     :FALSE
Wait for upgrade :FALSE
Support distr-upg :TRUE
Upgrade-banfwidth  :128
Upgrade group       :Upgrade-group1
```

AC IP(status)	acip ipv4 status of AP
AP IP(status)	apip ipv4 status of AP
AP IPV4 ENABLE	AP's apip ipv4 enable configuration
Location Data	Location information reported by the AP
Session ID	The session ID used by the AP to establish CAPWAP with the AC
mac type	MACTYPE type
WTP Name	AP name
AC Domain Name	AC domain name reported by the AP
wired vlan	wired-vlan configuration on AP LAN port 1
wired vlan	wired-vlan configuration on AP LAN port 2
wired vlan	wired-vlan configuration on AP LAN port 3
wired vlan	wired-vlan configuration on AP LAN port 4
Cw_interface_name	Selected interface name on AP

Cw_wan_interface_ifx	WAN port 1 index on AP
Cw_wan_interface_ifx	WAN port 2 index on AP
Upgrading State	AP upgrade status
AP Image file	AP upgrade bin name
Real version	The real version the AP is running
Custom version	The customized version of the software the AP is running
Upgrade version	AP upgraded version
Upgrade from AP	Whether to upgrade distributed from AP
Upgrade for other AP	Whether to do distributed upgrades for other APs
Upgrade from AC	Whether to upgrade from AC set
Wait for upgrade	Whether to wait for the upgrade
Support distr-upg	Whether to support distributed upgrade
Upgrade-banfwidth	Centrally upgrade bandwidth
Upgrade group	Centralized upgrade group

【Prompt Information】 -

【Platform Description】 -

4.55 show capwap detail

Use this command to display details about the CAPWAP

tunnel. show capwap [index| [ip-address[port]]] detail

【Parameter Description】

Parameter	Description
index	Tunnel index.
ip-address	Tunnel IP address.
port	Tunnel port number.

【Command Mode】 Privileged mode

【Default Level】 15

【Usage Guide】 -

【Configuration Example】 The following example displays details about the CAPWAP tunnel whose address is 1.1.1.1.

```
AC-FS#show capwap  1.1.1.1  detail
CAPWAP process "capwap 1" with state Run
  Process uptime is 3 days 0 hour 41 minutes
  Echo interval is 30 secs, Dead interval is 81 secs
  Current timers echo-interval
  Peer address is 172.18.59.5
  Peer control port is 10000, data port is 10001
  My address is 55.55.55.60
  The MAC of AP is 001a.a94e.d773
  The Session ID of AP is 001a.a94e.d773.53e1.0801.53e1.0801.53e1
  The Path MTU is 1500
  Recent recieved request's sequence number 39
  Recent recieved response's sequence number 11
  Recent send request's sequence number 11
  Retransmit Count 0, Discovery Count 0, Failed DTLS Session Count 0
  Sending queue length 0, Receive queue length 0
```

【Prompt Information】 -

【Platform Description】 -

4.56 show capwap state

Use this command to display the CAPWAP tunnel state.

show capwap state

【Parameter Description】 -

【Command Mode】 Privileged EXEC mode

【Default Level】 15

【Usage Guide】 -

【Configuration Examples】 The following example displays the CAPWAP tunnel state.

```
AC-FS#show capwap state
CAPWAP tunnel state, 3 peers, 2 is run:
Index  Peer IP                 Peer Port  State          Mac      Address
1.....192.168.0.1              10000      Run             001a.a900.0001
2      192.168.0.2             10000      Run             001a.a900.0002
3      192.168.0.3             10000      DTLS Teardown   001a.a900.0003
```

Field	Description
Index	Tunnel index.
Peer IP	Peer IP address.
Peer Port	Peer port number.
State	Tunnel state.
Mac Address	AP MAC address, only displayed on ACs.

【Prompt Information】 -

【Platform Description】 -

4.57 show capwap statistics

Use this command to display statistics about the CAPWAP tunnel packets.

show capwap [index| [ip-address[port]]] statistics

【Parameter Description】

Parameter	Description
index	tunnel index.
ip-address	IP address of the tunnel.
port	port number of the tunnel.

【Command Mode】 Privileged mode

【Default Level】 15

【Usage Guide】 -

【Configuration Examples】 The following example displays packet statistics about the CAPWAP tunnel whose IP address is 1.1.1.1.

```
AC-FS#show capwap 1.1.1.1 statistics
```

【Prompt Information】-

【Platform Description】 -

4.58 show version

Use this command to display the AP version.

show version { all |ap-name}

【Parameter Description】

Parameter	Description
all	All APs.
ap-name	Specify AP name.

【Command Mode】 Privileged mode

【Default Level】 15

【Usage Guide】 -

【Configuration Examples】 The following example displays the version information on all APs.

```
AC-FS#show version all
AP(AP220E-0)'s version:
  Product ID          : AP220-E
  System uptime       : 0:3:9:32
  Hardware version.....2.00
  Software version    : AP_RGOS 11.1(2)B1
```

```
  Patch number         : SP2
  Software number      : M05563609152014
  Serial number        : 1234942570005
  MAC address          : 00d0.f822.33b0

AP(AP220E-2)'s version:
  Product ID           : AP220-E
  System uptime        : 0:6:11:53
  Hardware version.....2.00
  Software version     : AP_RGOS 11.1(2)B1
  Patch number         : SP2
  Software number      : M05563609152014
  Serial number        : 1234942570018
  MAC address          : 001a.a9bd.0c1b
```

【Prompt Information】 -

【Platform Description】 -

4.59 slot

The configuration specifies the name of the AP card.

slot slot-id {slot-name [secondary] | mac mac-address slot-name }

Delete the name of the specified AP card.

no slot slot-id [{slot-name [secondary] | mac mac-address}]

【Parameter Description】

Parameter	Description
slot-id	Slot number, range 1~24.
slot-name	The name of the AP card, which can be configured with up to 63 characters and cannot contain spaces.
secondary	Slave micro APs deployed in cascade
mac-address	The mac address of the micro AP.

【Default Configuration】 By default, the AP card is not named.

【Command Mode】 AP configuration mode.

【Default Level】 15

【Usage Guide】 This command is only valid for Zhifen+AP devices, and does not support configuring all APs. The secondary Parameter needs to be added to the naming of the secondary micro APs deployed in cascade. Configure the micro-AP name based on the MAC address for offline configuration during construction. Each slot can be configured with two different MAC addresses. After the micro-AP corresponding to the MAC address goes online, it can be automatically converted to port-based according to the cascade relationship of the micro-AP. configuration.

【Configuration Example】1: The name of the micro AP1 configured with AP0001 is 1#101

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# slot 1 1#101
```

2: Configure the SLOT1 cascaded slave AP AP0001 as 1#102

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# slot 1 1#102 secondary
```

3: Configure the MAC address of SLOT1 as 0001.0001.0001 and the name of the micro AP as 1#101;

The micro AP with MAC address 0001.0001.0002 is named 1#102

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# slot 1 mac 0001.0001.0001 1#101
```

AC-FS(config-ap)# slot 1 mac 0001.0001.0002 1#102

【Verification】1: Use the show ap-config running command to view the configuration information of the corresponding AP.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.60 timestamp

Use this command to configure a specified AP or all APs in a specified AP group to synchronize with the AC in time.

Timestamp

【Parameter Description】 -

【Default Configuration】 -

【Command Mode】 AP configuration mode/AP group configuration mode

【Default Level】15

【Usage Guide】 -

【Configuration Examples】 1. The following example configures AP0001 to synchronize with the AC in time.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# timestamp
```

2: Configure the time for all APs in the AP group (Default) to synchronize this AC

```
AC-FS(config)# ap-group default
AC-FS(config-ap-group)# timestamp
```

【Prompt Information】-

【Platform Description】 -

4.61 tran-data-show

Displays various log information recently transmitted to the AC by the specified AP.

tran-data-show ap-name { exception | cpuinfo | memory | syslog | tech-support }

【Parameter Description】

Parameter	Description
ap-name	The name of the specified AP
exception	Specifies the AP's crash log information
cpuinfo	Specify the CPU information of the AP
memory	Specifies the memory information of the AP
syslog	Specifies the general information of the AP
tech-support	One-click collection of console information for specified APs

【Default Configuration】 -

【Command Mode】 AC configuration mode

【Default Level】15

【Usage Guide】 -

【Configuration Examples】 The following example displays the crash log of AP0001.

```
AC-FS(config-ac)# tran-data-show AP0001 exception
```

The following example displays the CPU information of AP0001.

```
AC-FS(config-ac)# tran-data-show AP0001 cpuinfo
```

The following example displays the memory information of AP0001.

```
AC-FS(config-ac)# tran-data-show AP0001 memory
```

The following example displays the general log information of AP0001.

```
AC-FS(config-ac)# tran-data-show AP0001 cpuinfo
```

The following example displays the console information of AP0001.

```
AC-FS(config-ac)# tran-data-show AP0001 tech-support
```

【Prompt Information】-

【Platform Description】 -

4.62 tran-data-start

Use this command to obtain log information about a specified AP.

tran-data-startap-name{ exception | memory | tech-support | tech-package }

【Parameter Description】

Parameter	Description
ap-name	Indicates the name of the specified AP.
exception	Indicates the crash log information sent by the specified AP.
memory	Indicates the device status information sent by the specified AP, including CPU information, memory information, and general log information (including port UP/DOWN information).
tech-support	Indicates the console information.
tech-package	Indicates the package information.

【Default Configuration】-

【Command Mode】 AC configuration mode

【Default Level】15

【Usage Guide】 -

【Configuration Examples】 The following example obtains the crash log information from AP0001, and saves it as ap_AP0001_exception.log in the AC file system.

```
AC-FS(config-ac)# tran-data-start AP0001 exception
```

The following example obtains the general log information from AP0001, and saves it as ap_AP0001_syslog.log, ap_AP0001_memory.log, and ap_AP0001_cpuinfo.log in the AC file system.

```
AC-FS(config-ac)# tran-data-start AP0001 memory
```

The following example obtains the console information from AP0001, and saves it as ap_AP0001_8832.0000.1111_tech-console.log in the AC file system.

```
AC-FS(config-ac)# tran-data-start AP0001 tech-support
```

The following example obtains the package information from AP0001, and saves it as ap_AP0001_8832.0000.1111_tech-package.tar.gz in the AC file system.

```
AC-FS(config-ac)# tran-data-start AP0001 tech-package
```

【Prompt Information】-

【Platform Description】 -

4.63 uninstall

Removes the specified micro AP installation information for the specified AP.

uninstall slot-id [secondary]

【Parameter Description】

Parameter	Description
slot-id	Slot number, range 1~24.
secondary	Slave micro APs deployed in cascade.

【Default Configuration】-

【Command Mode】 AP configuration mode

【Default Level】15

【Usage Guide】A micro AP has been installed in the designated slot of Zhifen+AP. If the micro AP is manually removed later, the system will consider the micro AP offline. This command can be used to remove the corresponding micro AP from the slot. If the micro AP in the slot is online, the command has no actual effect. This command does not save the configuration, and this command does not support configuring all APs.

The secondary Parameter needs to be added to the naming of the secondary micro APs deployed in cascade.

【Configuration Example】1: Remove the micro AP installation information in slot 1 of AP1.

```
AC-FS(config)# ap-config AP1
AC-FS(config-ap)# uninstall 1
```

2: Remove the cascading deployment of slot 1 of AP1 from the micro AP installation information.

```
AC-FS(config)# ap-config AP1
AC-FS(config-ap)# uninstall 1 secondary
```

【Verification】1: Use the show ap-config slot command to view the new micro AP installation information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.64 wired-interface

For APs with wired network interfaces (for example, wall-mounted RG-AP110-W APs provide an Ethernet port on the front of the product for wired network user access), the wired-interface command can be used to disable the above wired network interface. By default, the wired network interface is enabled.

wired-interface [slot slot-id] [port port-id] enable

Turn off the wired network interface:

no wired-interface [slot slot-id] [port port-id] enable

To restore the default configuration of the wired network interface on and off:

default wired-interface [slot slot-id] [port port-id] enable

【Parameter Description】

Parameter	Description
slot	Slot for micro AP access.
slot-id	Slot number, range 1~24.
port	Set up the wired network interface.
port-id	Specify the wired network interface, the value range is 1~4.
enable	Enable wired network interface.

【Default Configuration】The wired network port is enabled by default.

【Command Mode】AP Configuration Mode/All AP Configuration Mode/AP Group Configuration Mode

【Usage Guide】 1. This command can be configured for all APs, but the configuration is only valid for AP models with wired network interfaces.

2. When this command is configured without port Parameter, all wired network interfaces will be configured the same. When all four ports in the configuration are closed, the configuration is displayed without port Parameter. Slot Parameter is only valid for Zhifen+AP. If slot Parameter is not specified, the same configuration is applied to the 24-slot Micro AP.

3. The thin AP is started with zero configuration, and its configuration is delivered from the AC. The configuration information of the wired port is automatically saved on the AP. In this way, when the AP and AC are disconnected,

Restarting the AP will restore the configuration of the wired port. If the wired port is disabled, the wired port will still be closed after the

AP restarts.

When the wired port of the AP is closed, the AP cannot be managed through the wired port after restarting. At this time, you can long press the reset button of the AP to restore the factory configuration.

【Configuration Examples】 The following example disables the wired network port on AP1.

```
AC-FS(config)# ap-config AP1
AC-FS(config-ap)# no wired-interface
```

【Verification】 1: Use the show ap-config running command to check whether the configuration is successful.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

4.65 wired-vlan

For our AP with wired network interface (for example, the wall-mounted RG-AP110-W AP provides an Ethernet port on the front of the product for wired network user access), the wired-vlan command can be used to configure the above wired network interface VLAN to use. By default, the wired network interface uses the same VLAN as the AP.

wired-vlan vlan-Id [slot slot-id] [port port-id] auto-save

Restore Defaults.

no wired-vlan [vlan-id [slot slot-id] [port port-id]] auto-save

【Parameter Description】

Parameter	Description
vlan-id	Configure the VLAN used by the wired network interface. vlan-id: The specified VLAN, ranging from 1 to 4094.
slot	Slot for micro AP access.
slot-id	Slot number, range 1~24
port	Set up the wired network interface.
port-id	Specify the wired network interface, the value range is 1~4.
auto-save	Save the configuration on the AP and restore the configuration after the device

	restarts.

【Default Configuration】 The wired network port and the AP are in the same VLAN by default.

【Command Mode】 AP configuration mode/ AP group configuration mode

【Default Level】15

【Usage Guide】 1. This command can be configured for all APs, but the configuration is only valid for AP models with wired network interfaces.

2. When this command is configured without port Parameter, all wired network interfaces will be set to the same VLAN. When four ports are configured to belong to the same VLAN, the configuration displays without port Parameter. Slot Parameter is only valid for Zhifen+AP. If slot Parameter is not specified, the same configuration is applied to the 24-slot Micro AP.

3. In the wireless AP mode (the AP only performs wireless access and does not assign addresses to users), when the VLAN used by the wired network interface is configured to be the same as the AP, the VLAN to which the packets of the wired interface belong will be determined by the access switch, while Not the vlan specified in this configuration. When the packets of the wired network interface need to be forwarded with TAG, the native VLAN of the access switch cannot be the same as the VLAN of the wired network interface, otherwise the packets will not be forwarded to the wired network interface.

4. In wireless routing mode (AP can assign addresses to users), wired users will obtain addresses from the DHCP address pool on the AP, and the VLAN corresponding to the interface where the address pool is located must be the same as the VLAN specified by this command.

5. The thin AP is started with zero configuration, and its configuration is delivered from the AC. You can configure auto-save Parameter to automatically save the configuration information of the wired port on the AP. In this way, when the AP is disconnected from the AC, restarting the AP will restore the configuration of the wired port, so that users can still access the network through the wired port.

When the wired port configuration saving is enabled and the wired port VLAN is different from the native VLAN of the AP, if the AP cannot obtain the address after restarting, it will not be able to manage through the wired port. At this time, you can long press the reset button of the AP to restore the factory configuration.

【Configuration Example】1: Configure the wired network interface of AP1 to use VLAN 20.

```
AC-FS(config)# ap-config AP1
AC-FS(config-ap)# wired-vlan 20
```

【Verification】1: Use the show ap-config running command to check whether the configuration is successful.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5 WBS

5.1 11asuport enable

Configure the specified AP and specify the radio to support 11A under 5G.

11asupport enable radio radio-id

Configure the specified AP and the specified radio does not support 11A under 5G.

no 11asupport enable radio radio-id

【Parameter Description】

Parameter	Description
radio-id	Radio ID. The range is from 1 to 96.

【Default Configuration】 11A support.

【Command Mode】 AP configuration mode

【Default Level】 15

【Usage Guide】 The configuration takes effect only when the radio of the AP works under 5G.

【Configuration Examples】 1: Enter the AP0001 configuration mode, and configure Radio 1 to support 11A under 5G.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# 11asupport enable radio 1
```

【Verification】 1: Use the show ap-config running ap-name command to check whether the specified AP is configured to support 11A.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.2 11bsupport enable

Configure the specified AP and specify the radio to support 11 B under 2.4G.

11bsupport enable radio radio-id

Configure the specified AP and the specified radio does not support 11 B under 2.4G.

no 11bsupport enable radio radio-id

【Parameter Description】

Parameter	Description
radio-id	Radio ID. The range is from 1 to 96.

【Default Configuration】 11B support.

【Command Mode】 AP configuration mode

【Usage Guide】 The configuration takes effect only when the radio of the AP works under 2.4G.

【Configuration Examples】 1: Enter the AP0001 configuration mode, and configure Radio 1 to support 11B under 2.4G.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# 11bsupport enable radio 1
```

【Verification】1: Use the show ap-config running ap-name command to check whether the specified AP is configured to support 11B.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5.3 11gsupport enable

Configure the specified AP and specify the radio to support 11G under 2.4G.

11gsupport enable radio radio-id

Configure the specified AP and the specified radio does not support 11G under 2.4G.

no 11gsupport enable radio radio-id

【Parameter Description】

Parameter	Description
radio-id	Radio ID. The range is from 1 to 96.

【Default Configuration】 By default, 802.11g is supported.

【Command Mode】 AP configuration mode

【Default Level】 15

【Usage Guide】 The configuration takes effect only when the radio of the AP works under 2.4G.

【Configuration Examples】 1: Enter the AP0001 configuration mode, and configure Radio 1 to support 11G under 2.4G.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# 11gsupport enable radio 1
```

【Verification】 1: Use the show ap-config running ap-name command to check whether the specified AP is configured to support 11G.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.4 11nasupport enable

Configure the specified AP and the specified radio to support 11N under 5G.

11nasupport enable radio radio-id

Configure the specified AP and the specified radio does not support 11N under 5G.

no 11nasupport enable radio radio-id

【Parameter Description】 -

Parameter	Description
radio-id	Radio ID. The range is from 1 to 96.

【Default Configuration】 11N support.

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 The configuration only takes effect when the AP's Radio works under 5G.

【Configuration Examples】 1: Enter the AP0001 configuration mode, and configure Radio 1 to support 11N under 5G.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# 11nasupport enable radio 1
```

【Verification】1: Use the show ap-config running ap-name command to check whether the specified AP is configured to support 11N.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5.5 11ngsupport enable

Configure the specified AP and specify the radio to support 11N under 2.4G.

11ngsupport enable radio radio-id

Configure the specified AP and the specified radio does not support 11N under 2.4G.

no 11ngsupport enable radio radio-id

【Parameter Description】

Parameter	Description
radio-id	Radio ID. The range is from 1 to 96.

【Default Configuration】 Support 11N

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 N/A

【Configuration Examples】 1: Enter the AP0001 configuration mode, and configure Radio 1 to support 11N under 2.4G.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# 11ngsupport enable radio 1
```

【Verification】1: Use the show ap-config running ap-name command to check whether the specified AP is configured to support 11N.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5.6 11acsupport enable

Configure the specified AP and specify the radio to support 11AC.

11acsupport enable radio radio-id

Configure the specified AP and the specified radio does not support 11AC.

no 11acsupport enable radio radio-id

【Parameter Description】

Parameter	Description
radio-id	Radio ID. The range is from 1 to 96.

【Default Configuration】 Radios with an odd Radio ID do not support 11AC, and Radios with an even Radio ID support 11AC

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 N/A

【Configuration Examples】 1: Enter the AP0001 configuration mode, and configure Radio 1 to support 11AC.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# 11acsupport enable radio 1
```

【Verification】1: Use the show ap-config running ap-name command to check whether the specified AP is configured to support 11AC.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5.7 11axsupport enable

Configuration to specify that the AP Specifies that the radio supports 11AX

11axsupport enable radio radio-id\

Configure specify AP specified radio does not support 11AX.

no 11axsupport enable radio radio-id

Recover the specified AP specified radio with 11AX as Default Configuration.

default 11axsupport enable radio radio-id

【Parameter Description】

Parameter	Description
radio-id	Radio ID. The range is from 1 to 96.

【Default Configuration】 Radios with an odd Radio ID do not support 11AC, and Radios with an even Radio ID support 11AC

【Command Mode】 AP configuration mode

【Default Level】14

【Usage Guide】 -

【Configuration Examples】 1: Enter the AP0001 configuration mode, and configure Radio 1 to support 11AC.

```
AC-FS# configure terminal
AC-FS(config)# ap-config AP0001
```

【Verification】 Using the show ap-config running ap-name command, you can see if the specified AP has configured 11AX support.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

5.8 11ax-gi

Configuring the 11ax-gi parameter that the AP specifies radio.

11ax-gi { 0.8 | 1.6 | 3.2 | auto } radio radio-id

Restore the 11ax-gi parameter for the specified AP-specified radio.

no 11ax-gi radio radio-id

【Parameter Description】

Parameter	Description
radio-id	The id of the radio to be configured ranges from 1 to 96
0.8	Configure that the 11ax-gi is 0.8us
1.6	Configure that the 11ax-gi is 1.6us
3.2	Configure the 11ax-gi for 3.2us
auto	Configure 11ax-gi as auto, and the actual effective parameters are adaptive

【Default Configuration】 By default, 11ax-gi is the auto mode, and the actual effective parameters are adaptive.

【Command Mode】 AP configuration mode

【Default Level】14

【Usage Guide】 -

【Configuration Examples】 1: Enter the configuration mode of the AP0001, and the 11ax-gi of the configuration Radio 1 is 0.8us.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# 11ax-gi 0.8 radio 1
```

2: Enter the configuration mode of the AP0001, and restore the Radio 1 11ax-gi configuration.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# no 11ax-gi radio 1
```

【Verification】 Using the show ap-config running ap-name command, you can view the 11ax-gi configuration for the specified AP Radio.

【Prompt Information】 -

【Common Mistake】-

【Platform Description】 -

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 -

【Configuration Examples】 1: Enter the configuration mode of the AP0001, and the 11ax-gi of the configuration Radio 1 is 0.8us.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# 11ax-gi 0.8 radio 1
```

2: Enter the configuration mode of the AP0001, and restore the Radio 1 11ax-gi configuration.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# no 11ax-gi radio 1
```

【Verification】 Using the show ap-config running ap-name command, you can view the 11ax-gi configuration for the specified AP Radio.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.9 802.11a network rate

Configure the rate set supported by the 802.11a users.

802.11a network rate { 6 | 9 | 12 | 18 | 24 | 36 | 48 | 54 } { disabled | mandatory | supported }

【Parameter Description】

Parameter	Description
6	The rate is 6Mbps
9	The rate is 9Mbps
12	The rate is 12Mbps
18	The rate is 18Mbps
24	The rate is 24Mbps
36	The rate is 36Mbps
48	The rate is 48Mbps
54 disabled mandatory supported	The rate is 54Mbps not support must support optional support

【Default Configuration】 By default, rate 6Mbps, 12Mbps, 24Mbps must support, 9Mbps, 18Mbps, 36Mbps, 48Mbps, 54Mbps.

【Command Mode】 AC configuration mode、AP configuration、AP group configuration

【Default Level】 14

【Configuration Example】1: The 802.11a users disable the 6Mbps rate

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# 802.11a network rate 6 disabled
```

2: Configure the 802.11a users on the AP0001 to disable the 6Mbps rate.

```
AC-FS(config)# ap-config AP001
AC-FS(config-ap)# 802.11a network rate 6 disabled
```

3: Configure the 802.11a users on the default group to disable the 6Mbps rate.

```
FS(config)# ap-group default
AC-FS(config-group)# 802.11a network rate 6 disable
```

【Verification】 1: Use the show running command to view the configuration.

2: Using the show ap-config running ap-name command, you can view the configuration of the specified AP.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.10 802.11b network rate

Configure the rate set supported by the 802.11b users.

802.11b network rate { 1 | 2 | 5 | 11 } { disabled | mandatory | supported }

【Parameter Description】

Parameter	Description
1	Rate is 1Mbps.
2	Rate is 2Mbps.
5	Rate is 5.5Mbps.

11	Rate is 11Mbps.
disabled	Nonsupport.
mandatory	Must support.
supported	Option support.

【Default Configuration】 By default, rate 1Mbps, 2Mbps, 5.5Mbps, 11Mbps is must support

【Command Mode】 AC configuration、AP configuration mode、AP group configuration mode

【Default Level】 14

【Usage Guide】 -

【Configuration Examples】 1: The 802.11b user disables the 1Mbps rate

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# 802.11b network rate 1 disabled
```

2: Configure the 802.11b users on the AP0001 to disable the 1Mbps rate.

```
AC-FS(config)# ap-config AP001
AC-FS(config-ap)# 802.11b network rate 1 disabled
```

3: Configure the 802.11b users on the default group to disable the 1Mbps rate.

```
AC-FS(config)# ap-group default
AC-FS(config-group)# 802.11b network rate 1 disabled
```

【Verification】 1: Use the show running command to view the configuration.

2: Using the show ap-config running ap-name command, you can view the configuration of the specified AP.

【Prompt Information】 -

【Common Mistake】 -

5.11 802.11g network rate

Use this command to configure a RF rate list for the 802.11g network.

802.11g network rate { 1 | 2 | 5 | 6 | 9 | 11 | 12 | 18 | 24 | 36 | 48 | 54 } { disabled | mandatory | supported }

【Parameter Description】

Parameter	Description
1	Indicates 1Mbps rate.
2	Indicates 2Mbps rate.
5	Indicates 5Mbps rate.
6	Indicates 6Mbps rate.
9	Indicates 9Mbps rate.
11	Indicates 11Mbps rate.
12	Indicates 12Mbps rate.
18	Indicates 18Mbps rate.
24	The rate is 24Mbps.
36	The rate is 36Mbps.
48	The rate is 48Mbps.
54	The rate is 54Mbps.
disabled	not supported.
mandatory	must support.
supported	optional support.

【Default Configuration】 By default, the rates of 1Mbps, 2Mbps, 5.5Mbps, and 11Mbps are mandatory, and 6Mbps, 9Mbps, 12Mbps, 18Mbps, 24Mbps, 36Mbps, 48Mbps, and 54Mbps are optional.

【Command Mode】 AC configuration mode, AP configuration mode, AP group configuration mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example】 1: 802.11g users disable 1Mbps rate.

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# 802.11g network rate 1 disabled
```

2: Configure 802.11g users on AP0001 to disable 1Mbps rate.

```
AC-FS(config)# ap-config AP001
AC-FS(config-ap)# 802.11g network rate 1 disabled
```

3: Configure 802.11g users on the default group to disable the 1Mbps rate.

```
AC-FS(config)# ap-group default
AC-FS(config-group)# 802.11g network rate 1 disabled
```

【Verification】 1: Use the show running command to view the configuration.

2: Use the show ap-config running ap-name command to view the configuration of the specified AP.

【Prompt Information】 -

【Common Mistake】-

【Platform Description】-

5.12 {802.11a | 802.11b} network {enable | disable}

Use the { 802.11a | 802.11b } network { disable | enable } command to configure the switch status of the 2.4GHZ or 5GHZ network.

disable will cause all wireless users connected to 2.4GHZ or 5GHZ network in this wireless network to go offline.

{ 802.11a | 802.11b } network { enable | disable }

【Parameter Description】-

【Default Configuration】 The default is enable.

【Command Mode】 AC configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】 1: Configure 802.11a network disable.

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# 802.11a network disable
```

【Verification】1: Use the show running command to view the configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5.13 80.211n a-mpdu enable

Configure the specified AP to specify that the radio supports AMPDU.

802.11n a-mpdu enable radio radio-id

The configuration specified AP specified radio does not support AMPDU.

no 802.11n a-mpdu enable radio radio-id

【Parameter Description】

Parameter	Description
radio-id	Radio ID. The range is from 1 to 96.

【Default Configuration】 AMPDU is enabled by default.

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 This command takes effect only when the radio operates in 802.11n or 802.11ac.

【Configuration Examples】 1: Enter the AP0001 configuration mode, and configure Radio 1 to support AMPDU.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# 802.11n a-mpdu enable radio 1
```

【**Verification0** 1: Use the show ap-config running ap-name command to check whether the specified AP is configured to support AMPDU.

【**Prompt Information**】-

【**Common Mistake**】-

【**Platform Description**】-

5.14 80.211n mcs support

Configure the MCS of 11N that can be supported by the specified AP and the specified radio.

802.11n mcs support num radio radio-id

Restore the MCS of the maximum 11N supported by the specified radio of the specified AP.

no 802.11n mcs support radio radio-id

【**Parameter Description**】

Parameter	Description
num	MCS index. The range is from 0 to 31.
radio-id	Radio ID. The range is from 1 to 96.

【**Default Configuration**】 The default MCS index of 802.11n is 31.

【**Command Mode**】 AP configuration mode

【**Default Level**】 14

【**Usage Guide**】 N/A

【**Configuration Examples**】 The following example configures the MCS index to 15 of 802.11n for radio1.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# 802.11n mcs support 15 radio 1
```

【Verification】1: Use the show ap-config running ap-name command to check whether the specified AP is configured to support 11AC.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5.15 80.211ac mcs support

Configure the MCS of the maximum 11AC supported by the specified AP and the specified radio.

802.11ac mcs support num radio radio-id

Restore the MCS of the maximum 11AC supported by the specified radio of the specified AP.

no 802.11ac mcs support radio radio-id

【Parameter Description】

Parameter	Description
num	MCS index. The range is from 0 to 31.
radio-id	Radio ID. The range is from 1 to 96.

【Default Configuration】 The maximum supported default value of mcs of 11AC is 39。

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 N/A

【Configuration Examples】 1: Enter the AP0001 configuration mode, and configure the MCS of the 11AC supported by Radio 1 to be 19.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# 802.11ac mcs support 19 radio 1
```

【Verification】1: Use the show ap-config running ap-name command to check whether the specified AP is configured with a maximum supported MCS of 11AC.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5.16 802.11ax mcs support

Configure the MCS where the specified AP specifies the 11AX maximum that the radio supports.

802.11ax mcs support num radio radio-id

Restore MCS for the 11AX specified AP.

no 802.11ax mcs support radio radio-id

【Parameter Description】

Parameter	Description
times	Number of software retransmission, take the value range of 1-10.
radio-id	The id of the radio to be configured ranges from 1 to 96.

【Default Configuration】 The maximum supported MCS is 95.

【Command Mode】 AP configuration mode, all AP configuration modes

【Default Level】 14

【Usage Guide】 1. Configuration works only in AP radio works in 11AX mode.

2. The maximum mcs divided by 12 plus 1 indicates the number of spatial streams, such as if the configuration mcs is 31, the maximum number of spatial streams is 3 and the maximum mcs is 7.

【Configuration Examples】 Enter the configuration mode of AP0001 and the MCS of 11AX supported by Radio 2 is 9.

```
AC-FS# configure terminal
AC-FS(config)# ap-config AP0001
```

【Verification】 Use the show ap-config running ap-name command， can see if the specified AP configures the MCS for the

maximum supported 11AX.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

5.17 ampdu-retries

Configure the number of AMPDU software repasses that AP specifies radio.

ampdu-retries times radio radio-id

【Parameter Description】

Parameter	Description
time	The number of software retransmissions, the value range is 1-10
radio-id	The id of the radio to be configured ranges from 1 to 96.

【Default Configuration】 The AMPDU software retransmission number was 10.

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 Configuration only works on the Radio of the AP in 11N mode or 11AC mode. Configuring of all AP is not supported.

【Configuration Examples】 Enter the configuration mode of AP0001 and the AMPDU software retransmission of Radio 1 is 2.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# ampdu-retries 2 radio 1
```

【Verification】 1: Use the show ap-config running ap-name command to check whether the specified AP is configured with AMPDU software retransmission times.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.18 ampdu-rts

Configure the RTS protection mechanism that specifies AP specifies radio to the AMPDU aggregation message.

ampdu-rts radio { radio-id | 802.11b | 802.11a }

Configure the RTS protection mechanism that specifies that the AP specifies that the radio closes the AMPDU aggregation message.

no ampdu-rts radio { radio-id | 802.11b | 802.11a }

【Parameter Description】

Parameter	Description
radio-id	The id of the radio to be configured ranges from 1 to 96
802.11b	Configure all 2.4G radios
802.11a	Configure all 5.8G radios

【Default Configuration】 Disable

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 Specifying that the 802.11b parameter will configure all 2.4G radios，configuration takes effect when the AP is first launched and is automatically converted to a radio-based configuration；The same specified 802.11a parameter will configure all 5.8G radios, configuration takes effect when the AP is first launched and the command is automatically converted to a radio-based configuration. Configuration only works on the Radio of the AP in 11N mode or 11AC mode.

【Configuration Examples】 Enter the configuration mode of AP0001, and configure Radio 1 to open the RTS protection mechanism for AMPDU aggregate messages.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# ampdu-rts radio 1
```

【Verification】 1: Use the show ap-config running ap-name command to check whether the specified AP is configured to enable the RTS protection mechanism for AMPDU aggregation packets.

【Prompt Information】 -

【Common Mistake】 -

5.19 antenna receive

Configure the antenna receive type for the specified AP or all AP within the AP group.

antenna receive value radio radio-id

【Parameter Description】

Parameter	Description
value	Antenna selection mask, with the value range of: 1~255.
radio-id	The id of the radio to be configured ranges from 1 to 96.

【Default Configuration】 The AP configuration mode is designed for different product models and the number of different antennas, its default antenna selection mask is also different. Depending on each product model.

【Command Mode】 AP configuration mode or AP configuration mode

【Default Level】 14

【Usage Guide】 Configuration only works on the Radio of the AP in 11N mode or 11AC mode.

【Configuration Examples】 The configuration mode of the AP0001 is entered, and the receiving antenna of the configuration Radio 1 is set to 5.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# antenna receive 5 radio 1
```

2: Enter the AP group (default) configuration mode, and configure the receiving antenna of Radio 1 to be set to 5.

```
AC-FS(config)# ap-group default
AC-FS(config-group)# antenna receive 5 radio 1
```

【Verification】 1: Use the show ap-config running ap-name command, you can view the receiving antenna configuration for the specified AP Radio

2: Using the show running-config command, you can view the receive antenna configuration for the AP group Radio.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.20 antenna transmit

Configure the antenna send type for the specified AP or all AP within the specified AP group.

antenna transmit value radio radio-id

【Parameter Description】

Parameter	Description
value	Antenna selection mask, with the value range of: 1~255
radio-id	The id of the radio to be configured ranges from 1 to 96

【Default Configuration】 The AP configuration mode is designed for different product models and the number of different Antennas, its default antenna selection mask is also different. Depending on each product model.

The AP Group Configuration Mode is not configured by default

【Command Mode】 AP configuration mode or AP group configuration mode

【Default Level】 14

【Usage Guide】 Configuration only works on the Radio of the AP in 11N mode or 11AC mode.

【Configuration Examples】1: The configuration mode of the AP0001 is entered, and the transmission antenna of the configuration Radio 1 is set to 7.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# antenna transmit 7 radio 1
```

2: Enter the configuration mode of the AP group (default), and the transmission antenna of the configuration Radio 1 is set to 7.

```
AC-FS(config)# ap-group default
AC-FS(config-group)# antenna transmit 7 radio 1
```

【Verification】 1: Using the show ap-config running ap-name command, you can view the send antenna configuration for the specified AP Radio.

2: Using the show running-config command, you can view the transmission antenna configuration for the AP group Radio.

【Prompt Information】-

【Common Mistake】 -

【Platform Description】 -

5.21 antenna type

Configure the antennas of the specified AP or all AP specified radio within the specified AP group using a full directional or directional antenna.

antenna type { omnidirection | direction } [radio radio-id]

Configure the antenna type of the specified AP or all AP within the specified AP group uses Default Configuration.

no antenna type [radio radio-id]

Configure the antenna type of the specified AP or all AP within the specified AP group uses Default Configuration.

default antenna type [radio radio-id]

【Parameter Description】

Parameter	Description
omni direction	omni antenna.
direction	directional antenna.
radio-id	The id of the radio to be configured ranges from 1 to 96.

【Default Configuration】 omni antenna

【Command Mode】 AP configuration mode or AP group configuration mode

【Default Level】 14

【Usage Guide】 1: Configuration is valid only for radio that support both directional and directional antennas

2: If the built-in and external antenna can be switched, the configuration of the internal and external antenna will take priority, before the directional and directional configuration.

3: When the configuration does not specify the radio, it takes effect for all the radio s on the AP .

4: antenna type omnidirection and antenna type direction radio radio-id cannot be configured simultaneously on a specific group of ap \ ap \ all ap, later configured before override.

【Configuration Examples】 1: Enter the configuration mode of the AP0001, and configure the Radio 1 to use the orientation

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# antenna type direction radio 1
```

2: Enter the configuration mode of AP group (default) and all radio s use directional antenna.

```
AC-FS(config)# ap-group default
AC-FS(config-group)# antenna type direction
```

3: Enter the configuration mode of all AP and all radio 2 uses the directional antenna.

```
AC-FS(config)# ap-config all
AC-FS(config-ap)# antenna type direction radio 2
```

4: Configure all radio s and the specified radio cannot be configured simultaneously, the later configuration will override the preconfigured.

```
AC-FS(config)# ap-config AP0001 AC-FS(config-ap)# antenna type omnidirection
AC-FS(config-ap)# antenna type direction radio 1
AC-FS(config-ap)# antenna type direction radio 2 AC-FS(config-ap)# show ap-config running
!
ap-config AP0001
 antenna type direction radio 1
antenna type direction radio 2 // Post configured, override pre configuration and ultimately based on radio configuration
!
```

【Verification】1: Using the show ap-config running ap-name command, you can view the send antenna configuration for the specified AP

Radio

2: Using the show running-config command, you can view the transmission antenna configuration for the AP group Radio.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

5.22 apsd

The configuration specifies that the AP specifies whether the radio enables the U-APSD power-saving mode.

apsd { enable | disable } radio radio-id

【Parameter Description】

Parameter	Description
enable	Enable the U-APSD power-saving mode.
disable	Disable the U-APSD power-saving mode.
radio-id	The id of the radio to be configured ranges from 1 to 96.

【Default Configuration】 Enable the U-APSD power-saving mode

【Command Mode】 AP Configuration Mode

【Default Level】 14

【Usage Guide】 Configuring of all AP is not supported.

【Configuration Examples】 Enter the configuration mode of the AP0001, and the configuration Radio 1 enables the U-APSD power saving mode.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)#apsd enable radio 1
```

【Verification】 Use the show ap-config running ap-name command so that you can view the command configuration.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.23 ap-band-mode

Configure the frequency band mode for the specified AP

ap-band-mode {802.11a | 802.11b} radio [radio-id

【Parameter Description】

Parameter	Description
802.11a	Indicates the operating frequency band of 5G
802.11b	Indicates the operating frequency band of 2.4G
radio-id	The id of the radio to be configured, in the range of 1-96

【Default Configuration】 Depending on each product model.

【Command Mode】 AP Configuration

【Default Level】 14

【Usage Guide】 1: This configuration is an initial model setting, and the save configuration is not supported.

2: This configuration automatically restarts the AP device.

【Configuration Examples】 Enter the configuration mode of the ap680, and configure the Radio 3 to the 802.11a frequency band

```
AC-FS(config)# ap-config ap680
AC-FS(config-ap)#ap-band-mode 802.11a radio 3
Switch the band mode will auto reload system, continue?(Y/N) Y
```

【Verification】 After the AP automatically restarts， show ap-config summary view the working band of the AP corresponding to Radio.

【Prompt Information】-

【Common Mistake】 -

【Platform Description】 -

5.24 autowifi

Configure WLAN with one click on the empty configuration.

autowifi

Cancel the one-click configuration of WLAN.

no autowifi

【Parameter Description】 -

【Default Configuration】 -

【Command Mode】 AC global configuration mode

【Default Level】 14

【Usage Guide】 On devices with empty configuration, one-key configuration of WLAN is provided for quick configuration. It is generally used for rapid configuration by geological survey personnel to improve operation efficiency; it is convenient for channels to quickly configure WLAN for performance testing, etc.

【Configuration Examples】 The following example configures one-click WLAN configuration.

```
AC-FS(config)# autowifi
```

【Verification】1: Use the show running command to view the one-key configuration of WLAN.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5.25 assoc-rssi

Configure the minimum signal strength for wireless users of the specified AP to keep access to the specified radio.

assoc-rssi rssi radio radio-id

Restore the default minimum signal strength for wireless users of the specified AP's specified radio to keep access.

no assoc-rssi radio radio-id

【Parameter Description】

Parameter	Description
rssi	Specifies the RSSI. The range is from 0 to 100. The unit is dBm.
radio-id	Radio ID. The range is from 1 to 96.

【Default Configuration】 The default RSSI is 0, namely, the STA any RSSI can associate with the AP.

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 This command is used to clear sticky STAs in roaming scenario, It is recommended to set RSSI to a value in the range from 15 to 30.

【Configuration Examples】 The following example enters AP0001 configuration mode and sets the minimum RSSI for the STA.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# assoc-rssi 15 radio 1
```

【Verification】1: Use the show ap-config running ap-name command to view the configuration of the specified AP.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5.26 beacon dtim-period

Use this command to configure the period of delivery transmission indication messages (DTIM) for the specified radio.

beacon dtim-periodperiod-numradio radio-id

【Parameter Description】

Parameter	Description
period-num	DTIM period, which indicating the beacon periods. The range is from 1 to 255.
radio-id	Radio ID. The range is from 1 to 96.

【Default Configuration】 The default DTIM period is 1 (namely, 1 beacon period).

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 N/A

【Configuration Examples】 The following example configures the DTIM period of radio 1 of AP0001 to 30 beacon periods.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# beacon dtim-period 30 radio 1
```

【Verification】1: Use the show ap-config running ap-name command to view the configuration of this command.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5.27 beacon period

Use this command to configure the beacon period forthe specified radio of the specified AP.

beacon period milliseconds radio radio-id

【Parameter Description】

Parameter	Description
milliseconds	Period of sending Beacon frame, unit ms, range 20~1000.
radio-id	Radio ID. The range is from 1 to 96

【Default Configuration】 The default is beacon period is 100 milliseconds.

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 -

【Configuration Examples】 The following example configures the beacon period of radio 1 of AP0001 to 200 milliseconds.

```
AC-FS(config)# ap-configAP0001
AC-FS(config-ap)# beacon period200radio 1
```

【Verification】1: Use the show ap-config running ap-name command to check whether the specified AP is configured with the beacon frame sending period.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5.28 beacon rate

Configure the beacon frame sending rate of the specified AP's specified radio.

beacon rate rate-Mbps radio { radio-id | 802.11b | 802.11a }

Restore the beacon frame sending rate of the specified AP's specified radio to the default sending rate.

no beacon rate radio { radio-id | 802.11b | 802.11a }

【Parameter Description】

Parameter	Description
rate_Mbps	Beacon frame sending rate, it should be noted that: 1. If the rate is disabled by the rate set configuration, the rate cannot be configured; 2. Since the 5G frequency band does not support the rate of 1M/2M/5.5M/11M, if the radio is frequency band, the above rates cannot be configured;
radio-id	The id of the radio to be configured, ranging from 1 to 96
802.11b	Configure all 2.4G radios
802.11a	Configure all 5.8G radios

【Default Configuration】 The current command is not configured by default.

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 It specifies that 802.11b Parameter will configure all 2.4G radios. The configuration will take effect when the AP goes online for the first time and will be automatically converted to radio-based configuration; the same specified 802.11a Parameter will configure all 5.8G radio The configuration takes effect when the AP goes online for the first time, and the command is automatically converted to the radio-based configuration.

【Configuration Examples】 The following example configures the beacon rate of radio1 to 12Mbps.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# beacon rate 12.0 radio 1
```

【Verification】 1: Use the show ap-config running ap-name command to check whether the specified AP is configured with the beacon frame sending rate.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.29 chan-width

Configure the bandwidth of the specified radio of the specified AP.

chan-width { 20 | 40 | 80 | 160 } radio { radio-id | 802.11b | 802.11a }

【Parameter Description】

Parameter	Description
20	Configured for 20M bandwidth.
40	Configured for 40M bandwidth.
80	Configured for 80M bandwidth.
160	Configured for 160M bandwidth.
radio-id 802.11b 802.11a	The id of the radio to be configured, ranging from 1 to 96. Configure all 2.4G radios. Configure all 5.8G radios.

【Default Configuration】 The default channel bandwidth of 20 Mbps.

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 The specified 802.11b Parameter will configure all 2.4G radios. The configuration will take effect when the AP goes online for the first time and will be automatically converted to radio-based configuration; the same specified 802.11a Parameter will configure all 5.8G radios. The configuration takes effect when the AP goes online for the first time and the command is automatically converted to the radio-based configuration. Bandwidth configuration only takes effect when the AP works in 11N or 11AC mode.

【Configuration Examples】 1: Enter the AP0001 configuration mode, and configure the Radio 1 bandwidth to 40M.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# chan-width 40 radio 1
```

【Verification】1: Use the show ap-config running ap-name command to view the configuration information of the specified AP.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5.30 channel

Use this command to configure a channel for the specified radio of the specified AP.

channel { global | channel-id} radio radio-id

【Parameter Description】

Parameter	Description
chan-id	Specifies the channel ID.
global	Indicates that the channel is specified through the radio resource management (RRM) function.
radio-id	Sets radio ID. The range is from 1 to 48.

【Default Configuration】 By default, the channel is automatically adjusted by RRM.

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 1. It is not supported to configure all APs.

【Configuration Examples】 1: Enter the configuration mode of AP0001, and configure the working channel of Radio 1 as 6.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# channel 6 radio 1
```

【Verification】1: Use the show ap-config running ap-name command to view the configuration information of the specified AP.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5.31 channel-switch

Configure two radios of the same type specified by the specified AP to exchange channels.

channel-switch radio-id1 radio-id2

【Parameter Description】

Parameter	Description
radio-id1	The id of the first radio to exchange channels, the range is 1~96
radio-id2	The id of the second radio to exchange channels, in the range 1~96

【Default Configuration】 -

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 Configuring all APs is not supported.

Configuration of offline APs is not supported.

It is used when the third-frequency user access function is enabled.

This configuration is not saved, and the channel configuration is directly exchanged to save after configuration.

【Configuration Example】1: Enter the AP0001 configuration mode, and configure Radio 1 and 3 to switch working channels.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# channel-switch 1 3
```

【Verification】1: Use the show ap-config running ap-name command to view the configuration information of the specified AP.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5.32 country

The user can specify the set of country or region codes supported by the AC through the country command.

country country-code

The user can delete the country code supported by the AC through the country command.

no country country-code

The configuration specifies the country or region code used by the AP specified radio.

country country-code radio {radio-id | [802.11b | 802.11a]}

【Parameter Description】

Parameter	Description
country-code	Country code.
radio-id	Sets radio ID. The range is from 1 to 48.
802.11b	Configures radios on all 2.4 GHz frequency band.
802.11a	Configures radios on all 5.8 GHz frequency band.

【Default Configuration】 By default, the country code supported by an AC device is CN, and the country code used by an AP device is CN.

【Command Mode】 AP /AC configuration mode

【Default Level】 14

【Usage Guide】 1.The country code "CN" supported by an AC cannot be deleted.

2.This command cannot be configured for all APs at the same time.

3.There are two country codes available now: CN (China) and US (United States). The country code is divided into indoor (IN) and outdoor (OUT), Tag the country code with I or O to identify the environment. For example, CNI indicates China Indoor.

4. Before configuring a country code for an AP, add the country code to the country code set supported by the AC. If the country code used by an AP changes, the radio band, channel, and power of the AP change accordingly.

5. If 802.11b is specified, the country code is configured for all 2.4 GHz radios; the configuration takes effect when the AP goes online for the first time, and it takes effect on the specified radios only. When 802.11a is specified, the country code is configured for all 5.8 GHz radios; the configuration takes effect when the AP goes online for the first time and it takes effect on the specified radios only.

【Configuration Examples】 1: Configure the country or region code supported by the AC to be US, and configure the country or region code of radio 1 of AP0001 to be US.

```
AC-FS(config)# ac-controller AC-
FS(config-ac)# country US AC-
FS(config-ac)# exit AC-
FS(config)# ap-config AP0001
AC-FS(config-ap)# country US radio 1
```

【Verification】 1: Use the show running command to view the country code configuration supported by the AC.

2: Use the show ap-config running ap-name command to check whether the specified AP is configured with the country code.

【Prompt Information】 -

【Common Mistake】 1: The country code supported by the AC is not configured, directly configure AP Radio to use the country code.

```
AC-FS(config-ap)#country US radio 2
The country-code(US) is invalid, please check
```

【Platform Description】 -

5.33 country-code

Users can configure the country or region code for the AC with the country-code command.

country-code country-code

Users can recover the AC-supported country or regional code with the country-code command.

no country-code

【Parameter Description】

Parameter	Description
country-code	Country or regional code

【Default Configuration】 By default, the AC supports the national or regional code of "CN", the AP code is "CN"

【Command Mode】 Global configuration mode

【Defaults Level】 14

【Usage Guide】 1. After an AC configures the country or region code, all the AP on that AC will automatically use the country or region code for that AC configuration, if country code configuration also exists under radio.

2. The 102 country codes are currently supported:

Country count	Country or region
AE	United Arab Emirates
AM	Armenia
AR	Arg ntina
AT	Austria
AU	Australia
AZ	Azerbaijan
BE	Belgium
BG	Bulgaria
BH	Bahrain
BN	Brunei Darussalam
BO	Bolvia
BR	Brazil
BY	Belarus
EG	Egypt
BZ	Belize
CA	Canada
CH	Switzerl nd
CL	Chile
CN	China
CO	Colombia
CR	Costa Rica
CY	Cyprus
CZ	Czech Republic
DE	Germany
DK	Denmark
DO	Dominican Republic
EC	Ecuador
EE	Estonia
ES	Spain
FI	Finland

FR	France
GB	United Kingdom
ES	Spain
G	Georgia
GR	Greece
GT	Guatemala
HK	Hong Kong, Special Administrative Region of China
HN	Honduras
HR	Croatia
HU	Hungary
JO	Jordan
JP	Japan
KP	D.P.R.Korea
KR	R.O.Korea
KW	Kuwait
KZ	Kazakhstan
LB	Lebanon
LI	Liechtenstein
LK	Sri Lanka
LV	Latvia
MA	Morocco
MC	Monaco
MK	Macedonia
MO	Macao, Special Administrative Region of China
MT	Malta
MX	Mexico
MY	Malaysia
NG	Nigeria
NL	Netherlands
NO	Norway
NZ	New Zealand
OM	Oman
MO	Macao, Special Administrative Region of China
PA	Panama

PE	Peru

PH	Philippines
PK	Pakistan
PL	Poland
PR	Puerto Rico
PT	Portugal
QA	Qatar
RO	Romania
RU	Russia
SA	Saudi Arabia
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovak Republic
SV	El Salvador
SY	Syria
TH	Thailand
TN	Tunisia
TR	Turkey
TT	Trinidad & Tobago
TW	Taiwan, Province of China
UA	Ukraine
US	United States
PA	Panama
PE	Peru
PH	Philippines
UY	Uruguay
UZ	Uzbekistan
VE	Venezuela
VN	Vietnam
YE	Yemen
ZA	South Africa
ZW	Zimbabwe

3. When the country or region code used by AP changes, the RF frequency band, channel and power value corresponding to AP will also change.

4. 2.4G does not support channel 14.

【Configuration Example】 1: The country or region code for configuring the AC is the US.

```
AC-FS(config)# AC-FS(config)# country-code US
AC-FS(config)# exit
```

【Verification】 Using the show running command, you can view the AC-supported country code configuration.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.34 coverage-area-control

Configure the AP management frame power selection.

coverage-area-control power [radio { radio-id | 802.11b | 802.11a }]

Restore the AP management frame power selection.

no coverage-area-control [radio { radio-id | 802.11b | 802.11a }]

【Parameter Description】

Parameter	Description
power	Manage frame power in dbm, range of 0~32..
radio-id	Management frame power, unit: dbm, range 0~32.
802.11b	The id of the radio to configure, in the range 1-96.
802.11a	Configure all 2.4G radios.

【Default Configuration】 0

【Command Mode】 AP configuration mode、AP group configuration mode

【Defaults Level】 14

【Usage Guide】 Specifying that the 802.11b parameter will configure all 2.4G radios, Configuration takes effect when the AP is first launched and is automatically converted to a radio-based configuration; The same specified 802.11a parameter will configure all 5.8G radios, configuration takes effect when the AP is first launched and the command is automatically converted to a radio-based configuration.

【Configuration Example】1: Enter the AP0001 configuration mode, and configure the AP management frame power to be 20.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# coverage-area-control 20
```

2: Enter the AP group (default) configuration mode, and configure the AP management frame power to 20.

```
AC-FS(config)# ap-group default
AC-FS(config-group)# coverage-area-control 20
```

【Verification】1: Use the show ap-config running ap-name command to check whether the specified AP is configured with management frame power selection.

1: Use the show running-config command to view the AP group management frame power configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】

5.35 enable-radio

Set the enabling state for the radio or all radio s of the specified AP to open.

enable-radio { radio-id | all }

Set the enabling state for the radio or all radio of the specified AP to close.

no enable-radio { radio-id | all }

【Parameter Description】

Parameter	Description
radio-id	The id of the radio to be configured, ranging from 1 to 96.
all	Refers to all radios.

【Default Configuration】 By default, all radio for all AP are enabled.

【Command Mode】 AP configuration mode

【Defaults Level】 14

【Usage Guide】 This operation causes all wireless users connected to the radio specified to be offline. Configuring of all AP is not supported.

【Configuration Example】 Enter the configuration mode of the AP0001, and the configuration Radio 1 status is off.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# no enable-radio 1
```

【Verification】 Use the show ap-config running ap-name command to view the specified AP Radio enabling configuration.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.36 external-antenna enable

Configuration Specifies that the AP Specifies that the radio enables an external antenna, and disables the built-in antenna.

external-antenna enable radio radio-id

Restover the specified AP Specifies radio enables the built-in antenna and disables the external antenna.

no external-antenna enable radio radio-id

【Parameter Description】

Parameter	Description
radio-id	The id of the radio to be configured ranges from 1 to 96.

【Default Configuration】 By default, enable the built-in antenna and disabled the external antenna.

【Command Mode】 AP configuration mode

【Default Level】14

【Usage Guide】 -

【Configuration Example】 Enter the AP0001 configuration mode, and configure the Radio 1 to enable the external antenna, and disable the built-in antenna.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# external-antenna enable radio 1
```

【Verification】 Using the show ap-config running ap-name command, you can see if the specified AP Radio is configured to enable the external antenna, and to disable the built-in antenna.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.37 extra-coverage

Configure the AP to open the user access function of the third frequency.

extra-coverage enable

Configure the AP to turn off the user access function of the third frequency.

no extra-coverage enable

The user access function to restore the AP third frequency is Default Configuration.

default extra-coverage enable

【Parameter Description】 -

【Default Configuration】 By default, the user access function of the third frequency is turned off.

【Command Mode】 AP configuration, AP group configuration mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example】 1: Enter the configuration mode of the AP0001 and activate the user access function of the third frequency.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# extra-coverage enable
```

2: Enter the configuration mode of the AP0001, and configure the user access function for closing the third frequency.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# no extra-coverage enable
```

3: The configuration mode of AP0001 and the user access function restoring the third frequency is Default Configuration.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# default extra-coverage enable
```

【Verification】 Using the show ap-config running ap-name command, you can view the user access function configuration for the specified AP third frequency.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.38 fragment-threshold

Configure the fragmentation threshold of the specified radio of the specified AP.

fragment-threshold value radio radio-id

Restores the fragmentation threshold of the specified radio of the specified AP to the default value.

no fragment-threshold radio radio-id

【Parameter Description】

Parameter	Description
value	The configured shard threshold, an even number between 256 and 2346.
radio-id	The id of the radio to be configured, ranging from 1 to 96.

【Default Configuration】 By default, the fragmentation threshold is 2346.

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】Does not support configuring all APs.

【Configuration Example】1: Enter the AP0001 configuration mode, and configure the fragmentation threshold of Radio 1 to be 1538.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# fragment-threshold 1538  radio 1
```

【Verification】1: Use the show ap-config running ap-name command to view the configuration of the specified AP fragmentation threshold.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5.39 green-field enable

Configure the protection mode of the specified radio of the specified AP.

green-field enable radio radio-id

Restore the protection mode of the specified radio of the specified AP to disable.

no green-field enable radio radio-id

【Parameter Description】

Parameter	Description
radio-id	The id of the radio to be configured, ranging from 1 to 96.

【Default Configuration】 The default is disable.

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 Only supports 2.4G Radio.

【Configuration Example】1: Enter the configuration mode of AP0001, and configure the green-field protection mode of Radio 1.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# green-field enable radio 1
```

【Verification】1: Use the show ap-config running ap-name command to view the green-field configuration of the specified AP Radio.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5.40 hap-poe enable radio

Switthe AP power power RF.

hap-poe enable radio {802.11a | 802.11b}

Working RF when the AP supply is insufficient.

default hap-poe enable

【Parameter Description】

Parameter	Description
802.11a	When the power supply is insufficient, switch to 5G operation.
802.11b	When the power supply is insufficient, switch to 2.4G operation.

【Default Configuration】 Default selects the working RF based on the AP capability values.

【Command Mode】 AP configuration mode, AP group configuration mode and all AP configuration modes

【Default Level】 14

【Usage Guide】 The AP that needs to distinguish operating RF takes effective only if power supply is insufficient, and if power is sufficient, the working RF is not limited after configuration.

【Configuration Example】 Enter the configuration mode of AP0001 and configure insufficient power supply to work with

5G RF.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# hap-poe enable radio 802.11a
```

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.41 ldpc

Configure the specified AP to specify that the radio supports low-density parity check encoding.

ldpc radio radio-id

Configure the specified AP and the specified radio does not support LDPC encoding.

no ldpc radio radio-id

【Parameter Description】

Parameter	Description
radio-id	The id of the radio to be configured, ranging from 1 to 96.

【Default Configuration】 support

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example】 The following example enters the configuration mode of AP0001 and enables LDPC coding on radio 1.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# ldpc radio 1
```

【Verification】1: Use the show ap-config running ap-name command to check whether the specified AP is configured to support LDPC encoding.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5.42 link-check

Enable or disable link integrity detection.

link-check { enable | disable }

Enable or disable link integrity detection.

no link-check { enable | disable }

【Parameter Description】

Parameter	Description
no	inverse operation.

【Default Configuration】 closure

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example】 The following example enables link check.

```
FS(config)# link-check disable
FS(config)# no link-check enable
```

【Configuration Example】1: Enable the link integrity detection function.

```
AC-FS(config)# link-check enable
```

2: Disable the link integrity detection function.

```
AC-FS(config)# link-check disable
```

or

```
AC-FS(config)# no link-check enable
```

【Verification】1: Use the show running-config command to check the status of the link integrity detection function being enabled.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5.43 linktest

Use this command to display the link information about a wireless client.

linktestH.H.H

【Parameter Description】

Parameter	Description
H.H.H	Client's MAC address.

【Command Mode】 Privileged mode

【Default Level】 1

【Usage Guide】 -

【Configuration Example】 1: Display wireless user (MAC address: cca2.2352.768d) link information

```
AC-FS# linktest cca2.2352.768d
Link test station(cca2.2352.768d):
    Signal strength in the form of RSSI :           55
    Signal quality in the form of SNR-------------------------37
    Total number of packets that are retried:       9
    Maximum retry count for a single packet:        16
    Number of lost packets:                         0
    Data rate of a successfully transmitted packet: 0
```

Field	Description
Signal strength in the form of RSSI	Signal strength in the form of a received signal strength indication.
Signal quality in the form of SNR	Signal quality in terms of signal-to-noise ratio.
Total number of packets that are retried	Total number of retransmitted frames.
Maximum retry count for a single packet	Maximum number of retransmissions of a single packet.
Number of lost packets	total packet loss.
Data rate of a successfully transmitted packet	The rate at which packets are successfully transmitted.

【Prompt Information】-

【Platform Description】-

5.44 mcast-rate

Configure the multicast rate of the WLAN.

mcast-rate mcast-num

Restore the multicast rate of the WLAN to the default value.

no mcast-rate

【Parameter Description】

Parameter	Description
mcast-num	WLAN multicast rate. The available rates: 1Mbps, 6Mbps, 11Mbps, 24Mbps, 54Mbps.

【Default Configuration】 The default WLAN multicast rate is 24Mbps.

【Command Mode】 WLAN configuration mode

【Usage Guide】 -

【Configuration Example】 The following example configures the multicast rate of WLAN2048 to 11Mbps.

```
AC-FS(config)# wlan-config 2048
AC-FS(config-wlan)# mcast-rate 11
```

【Verification】1: Use the show running-config command to view the multicast rate configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5.45 mcell

Configure the specified AP and the specified radio to enable the mcell function.

mcell enable radio radio-id

Configure the specified AP and the specified radio to disable the mcell function.

no mcell enable radio radio-id

【Parameter Description】

Parameter	Description
radio-id	The id of the radio to be configured, ranging from 1 to 96.

【Default Configuration】Close

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Enter the AP0001 configuration mode, and configure Radio 1 to enable the mcell function.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# mcell enable radio 1
```

【Verification】1: Use the show ap-config running ap-name command to check whether the mcell function is enabled on the specified AP.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5.46 mu-mimo enable

Configure the specified radio to enable the MU-MIMO function.

mu-mimo enable radio radio-id

Configure the specified radio to disable the MU-MIMO function.

no mu-mimo enable radio radio-id

Restore the MU-MIMO function of the specified radio.

default mu-mimo enable radio radio-id

【Parameter Description】

Parameter	Description
radio-id	The id of the radio to be configured, ranging from 1 to 96.

【Default Configuration】 Open by default.

【Command Mode】AP configuration mode, all AP configuration mode, AP group configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Enter the AP0001 configuration mode, and configure Radio 1 to enable MU-MIMO.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# mu-mimo enable radio 1
```

2: Enter the AP0001 configuration mode, and configure Radio 2 to disable MU-MIMO.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# no mu-mimo enable radio 2
```

3: Enter the configuration mode of AP0001 and restore the default MU-MIMO of Radio 3.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# default mu-mimo enable radio 3
```

4: Enter the AP all configuration mode, configure Radio 1 to enable MU-MIMO.

```
AC-FS(config)# ap-config all
AC-FS(config-ap)# mu-mimo enable radio 1
```

5: Enter the AP default configuration mode, configure Radio 1 to enable MU-MIMO.

```
AC-FS(config)# ap-group default
AC-FS(config-group)# mu-mimo enable radio 1
```

【Verification】1: Use the show ap-config running ap-name command to view the MU-MIMO configuration of the specified AP Radio.

2: Use the show running-config command to view the MU-MIMO configuration of the AP group Radio.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5.47 ofdma enable

Configuration specifies that the radio turns on the OFDMA functionality.

ofdma enable radio radio-id

Configure specifies that the radio turns off the OFDMA functionality.

no ofdma enable radio radio-id

【Parameter Description】

Parameter	Description
radio-id	The id of the radio to be configured ranges from 1 to 96.

【Default Configuration】 Defaults open

【Command Mode】 AP configuration mode, all AP configuration mode, AP group configuration mode

【Default Level】 14

【Usage Guide】 Radio support OFDMA to configure, and radio that does not support OFDMA does not support OFDMA.

【Configuration Example】 1: Enter the configuration mode of the AP0001, and configure the Radio 2 to close the OFDMA.

```
AC-FS# configure terminal
AC-FS(config)# ap-config AP0001
```

2: The radio configuration mode of ofall is turned off.

```
AC-FS# configure terminal AC-
FS(config)# ap-config all
AC-FS(config-ap)# no ofdma enable radio 2
```

3: Enter the AP group default configuration mode, configure Radio 2 to disable OFDMA.

```
AC-FS# configure terminal AC-
FS(config)# ap-group default
AC-FS(config-group)# no ofdma enable radio 2
```

【Verification】 1: Use the show ap-config running ap-name command to view the OFDMA configuration of the specified AP adio.

2: Use the show running-config command to view the OFDMA configuration of the AP group radio.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

5.48 peer-distance

Use this command to configure the maximum distance between the specified radio and the peer. peer-distance valradio radio-id default mu-mimo enable radioradio-id

【Parameter Description】

Parameter	Description
val	To configure the maximum distance allowed by the AP, the value range is 1000~25000, unit: m
radio-id	Radio ID. The range is from 1 to 48.

【Default Configuration】 The default distance between the radio and the peer is 1,000 meters.

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】Configuring all APs is not supported. Configuration is only required when the farthest distance between the AP and the wireless transmission peer is greater than 1000m. The configured distance can be larger but not smaller than the actual distance.

【Configuration Example】 1: Enter the configuration mode of AP0001, and configure the maximum distance between Radio 1 and the wireless transmission peer to be 3000m.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# peer-distance 3000 radio 1
```

【Verification】1: Use the show ap-config running ap-name command to view the configuration of the longest distance allowed between the specified AP Radio and the wireless transmission peer.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5.49 power local

Use this command to configure trasmit power for the specified radio of the specified AP. power local { global |power} radio { radio-id|[802.11b| 802.11a] }

【Parameter Description】

Parameter	Description
power	Indicates the percentage of transmit power. The range is from 1 to 100.
Global	Indicates that the transmit power is specified through RRM for the specified AP or all APs of the specified AP group.
radio-id	Radio ID. The range is from 1 to 48.
802.11b	Configures 2.4GHz radio.
802.11a	Configures 5.8GHz radio.

【Default Configuration】 By default, the transmit power is automatically adjusted by RRM

【Command Mode】 AP configuration mode/AP group configuration mode

【Default Level】 14

【Usage Guide】 It specifies that 802.11b Parameter will configure all 2.4G radios. The configuration will take effect when the AP goes online for the first time and will be automatically converted to radio-based configuration; the same specified 802.11a Parameter will configure all 5.8G radio. The configuration takes effect when the AP goes online for the first time, and the command is automatically converted to the radio-based configuration. Configuring all APs is not supported.

【Configuration Example】 1. The following example configures the transmit power of radio1 of AP0001 to 50%.

```
AC-FS(config)# ap-configAP0001
AC-FS(config-ap)# power local50radio 1
```

2. The following example configures the transmit power of radio 1 of AP group (default) to 50%.

```
AC-FS(config)# ap-group default
AC-FS(config-group)# power local 50 radio 1
```

【Verification】1: Use the show ap-config running ap-name command to view the transmit power configuration of the specified AP Radio.

2: Use the show running-config command to view the radio transmit power configuration of the AP group.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5.50 preamable

Use this command configure the preamable attribute for the specified radio of the specified AP.

preamable { long | short } radioradio-id

【Parameter Description】

Parameter	Description
radio-id	The id of the radio to be configured, ranging from 1 to 96.
long	Specifies that the AP only transmits frames with long preambles.
short	Specifies that the AP can transmit frames with a short or long preamble.

【Default Configuration】 By default, it is short, that is, the short preamble is used.

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】Does not support configuring all APs.

【Configuration Example】1: Enter the AP0001 configuration mode, and configure Radio 1 to disable the short preamable function.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# preamble long radio 1
```

【Verification】1: Use the show ap-config running ap-name command to view the short preamable configuration of the specified AP Radio.

【Prompt Information】-

【Common Mistake】-

5.51 poe-unlimit

In the case of the power supply negotiation limit, the AP is forced to release the limit to ensure that the AP can configure the command of the maximum capability attribute.

poe-unlimit [radio radio-id | radio-type { 802.11a | 802.11b }]

【Parameter Description】

Parameter	Description
radio-id	The id of the radio to be configured, ranging from 1 to 96.
long	Indicates the operating frequency band of 5GHZ.
short	Indicates the working frequency band of 2.4GHZ.

【Default Configuration】 By default, the limit is based on the power supply negotiation result.

【Command Mode】 AP configuration mode

【Default Level】

【Usage Guide】 Does not support configuring all APs.

【Configuration Example】 1: Enter the AP0001 configuration mode, and configure Radio 1 to disable the power supply limit function.

```
AC-FS(config-ap)# poe-unlimit radio 1
AC-FS(config-ap)# poe-unlimit radio-type 802.11a
```

【Verification】 1: Use the show ap-config running ap-name command to view the configuration of the poe-unlimit of the specified AP Radio.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.52 radio-optimize

One-click recommended configuration to specify the radio parameters of the AP (including power, channel, and antenna transceiver type).

radio-optimize [{ 802.11a | 802.11b } { 802.11a | 802.11b }]

【Parameter Description】

Parameter	Description
802.11a	802.11a indicates the working frequency band of 5GHZ.
802.11b	802.11b indicates the working frequency band of 2.4GHZ.

【Default Configuration】 By default, one-key recommended configuration is not performed.

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 1. It is not supported to configure all APs.

2. If the corresponding AP is offline, only optimization is supported, and it is not supported to change the radio-type in this command (if you need to change the radio-type, please use it directly.

radio-type command), the configuration will be saved after optimization and processed when the AP goes online.

3. If the corresponding AP is online, it supports changing the radio-type and optimizing at the same time. It supports the direct optimization based on the current radio-type without changing the radio-type; according to the AP support capability, the AP that does not support the one-key recommended configuration is not processed. For APs that support one-click recommended configuration, immediately change the radio parameters (including power, channel, and antenna transceiver type) and no longer save this configuration (relevant parameters are saved by themselves).

【Configuration Example】1: Enter the configuration mode of AP0001, and configure the one-click recommended configuration.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# radio-optimize
```

2: Enter the online AP0002 configuration mode, and change the radio-type through one-key recommended configuration.

```
AC-FS(config)# ap-config AP0002
AC-FS(config-ap)# radio-optimize 802.11a 802.11a
```

【Verification】1: Use the show ap-config running ap-name command to view the radio Parameter configuration of the specified AP (the online AP can directly view the relevant radio Parameter configuration, and the offline AP can check whether the one-key recommended configuration is enabled).

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5.53 radio-type

Use this command to configure the RF mode for the specified radio of the specified AP.

radio-typeradio-id{802.11a | 802.11b}

【Parameter Description】

Parameter	Description
radio-id	Radio ID. The range is from 1 to 48.
802.11a	Indicates the 5GHz band is used.
802.11b	Indicates the 2.4GHz band is used.

【Default Configuration】 By default, the AP device with single radio (namely, radio1) operates in 2.4 GHz, while the AP device with dual radios can operate in 2.4 GHz (radio1) and 5 GHz (radio2).

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 Does not support configuring all APs.

【Configuration Example】 1: Enter the AP0001 configuration mode, and configure Radio 1 to work in the 2.4G frequency band.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# radio-type 1 802.11a
```

【Verification】1: Use the show ap-config running ap-name command to view the working frequency band configuration of the specified AP Radio.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5.54 response-rssi

Configure the specified AP and specify the minimum signal strength of the radio that allows access to wireless users.

response-rssi rssi radio { radio-id | 802.11b | 802.11a }

Restore the minimum signal strength of the specified AP and the specified radio to allow access to wireless users to the default value.

no response-rssi radio radio-id

【Parameter Description】

Parameter	Description
rssi	Specifies the RSSI. The range is from 0 to 100. The unit is dBm.
radio-id	Radio ID. The range is from 1 to 96.
802.11b	Configures radios on all 2.4 GHz frequency band.
802.11a	Configures radios on all 5.8 GHz frequency band.

【Default Configuration】 By default, it is 0, that is, all wireless users with signal strength are allowed to access.

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】The specified 802.11b Parameter will configure all 2.4G radios. The configuration will take effect when the AP goes online for the first time and will be automatically converted to radio-based configuration; the same specified 802.11a Parameter will configure all 5.8G radios. The configuration takes effect when the AP goes online for the first time and the command is automatically converted to the radio-based configuration.

【Configuration Example】 1: Enter the AP0001 configuration mode, and configure Radio 1 to allow access to wireless users with a minimum signal strength of 20

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# response-rssi 20 radio 1
```

【Verification】1: Use the show ap-config running ap-name command to view the configuration of the specified AP.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5.55 rts-threshold

Configure the RTS threshold of the specified radio of the specified AP.

rts-threshold value radio radio-id

Restore the RTS threshold of the specified radio of the specified AP to the default value.

no rts-threshold radio radio-id

【Parameter Description】

Parameter	Description
value	RTS threshold. The unit is byte. The range is from 257 to 2,347.
radio-id	Radio ID. The range is from 1 to 96.

【Default Configuration】 The default RTS threshold is 2,347.

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 N/A

【Configuration Example】 The following example configures the RTS threshold of radio1 to 1,539.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# rts-threshold 1539 radio 1
```

【Verification】1: Use the show ap-config running ap-name command to view the RTS threshold configuration of the specified AP Radio.

【Prompt Information】-

5.56 short-gi

Configure the specified AP and the specified radio to support short-gi.

short-gi enable radio radio-id chan-width { 20 | 40 | 80 | 160}

Configure the specified AP and the specified radio does not support short-gi.

no short-gi enable radio radio-id chan-width { 20 | 40 | 80 | 160}

【Parameter Description】

Parameter	Description
radio-id	The id of the radio to be configured, ranging from 1 to 96.
20	Configured for 20M bandwidth.
40	Configured for 40M bandwidth.
80	Configured for 80M bandwidth.
160	Configured for 160M bandwidth.
radio-id	The id of the radio to be configured, ranging from 1 to 96.

【Default Configuration】 By default, 20Mbps, 40Mbps, 80Mbps and 160Mbps are enabled.

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example】1: Enter AP0001 configuration mode, and configure Radio 1 to support short-gi with 20M bandwidth.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# short-gi enable radio 1 chan-width 20
```

2: Enter the configuration mode of AP0001, and configure Radio 2 to not support short-gi with 40M bandwidth.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# no short-gi enable radio 2 chan-width 40
```

【Verification】1: Use the show ap-config running ap-name command to view the short-gi configuration of the specified AP Radio.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5.57 short-slot-time

Use this command to enable short slot time for the AP device. Use the no form of this command to disable short slot time.

short-slot-time

radioradio-id no short-slot-time radioradio-id

【Parameter Description】

Parameter	Description
radio-id	The id of the radio to be configured, ranging from 1 to 96.

【Default Configuration】 By default, it is enable.

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 The long slot time does not take effect when the radio of the AP works under 5G.

【Configuration Example】 1: Enter the AP0001 configuration mode, and configure Radio 1 to support the short slot time function.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# short-slot-time radio 1
```

【Verification】1: Use the show ap-config running ap-name command to view the short-slot-time configuration of the specified AP Radio.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5.58 stbc

Configure the specified AP to enable the specified radio to receive and transmit space-time block codes.

stbc radio radio-id

Configure the specified AP and the specified radio to prohibit receiving and sending space-time block codes.

no stbc radio radio-id

【Parameter Description】

Parameter	Description
radio-id	The id of the radio to be configured, ranging from 1 to 96.

【Default Configuration】 Enable

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example】1: Enter the AP0001 configuration mode, and configure Radio 1 to enable receiving and sending space-time block codes.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# stbc radio 1
```

【Verification】1: Use the show ap-config running ap-name command to check whether the specified AP is configured to enable receiving and sending space-time block codes.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

5.59 show ac-config { 802.11a | 802.11b } summary

Use this command to display the AP devices supporting in 802.11a/b on the AC device.

show ac-config { 802.11a | 802.11b } summary

【Parameter Description】 -

【Default Configuration】 -

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】 -

【Configuration Example】 1: Display the list of APs in the 802.11a network of this AC.

```
AC-FS#show ac-config 802.11a summary
Index  Ap name                              slot id Radio Base MAC state load(%)
noise(dBm) interfere(%)

1      ap320v1.0                            2       0000.0000.0000  Enable   0----------110
0
2      00d0.fb88.7812                       2       00d0.fb88.7815  Enable   0----------110
0
```

Field	Description
Index	serial number.
Ap name	AP name.
slot id	radio id.
Radio Base MAC	radio MAC address.
state	enable/disable state.
load(%)	channel load.
noise(dBm)	noise floor.
interfere(%)	Co-channel interference.

【Prompt Information】-

【Platform Description】-

5.60 show ap-config radio

Use this command to display the radio configuration of all APs .

show ap-config radio

【Parameter Description】 -

【Default Configuration】 -

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】 -

【Configuration Example】1: View the radio information of all APs

```
AC-FS#show ap-config radio
Show all AP radios:
```

```
   AP Name                          MAC Address        Radio MAC          Radio MAC
-------------------------------------------------------------------------------------------

     AP0001                          N/A                N/A                N/A
```

Field	Description
AP Name	AP name.
MAC Address	AP MAC address.
Radio MAC	Radio MAC address with an odd radio ID.
Radio MAC	Radio MAC address with an even number of Radio IDs.

【Prompt Information】-

【Platform Description】-

5.61 show ap-config radio ap-name

Use this command to display the radio configuration of all APs.

show ap-config radio ap-nameap-name

【Parameter Description】

Parameter	Description
ap-name	Specify the name of the AP to be queried.

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】 -

【Configuration Example】 1: View the radio information of all APs.

```
AC-FS#show ap-config radio ap-name
Radio ID Radio Type      STA NUM  Channel  Power  Radio Base MAC  Status
________ _______________ _______ ________ ______ ______________ _______

1        802.11b/g/n     10       6*       100    000c.3067.fbd7  Enable
2.....802.11a/n/ac/ax  0        149*     100    000c.3067.fbd8  Disable
```

Field	Description
Radio ID	RF Interface ID.
Radio Type	Working frequency.
STA NUM	Number of STAs.
Channel	channel.
Power	power.
Radio Base MAC	The mac address of the radio port.
Status	RF port status.

【Prompt Information】-

【Platform Description】-

5.62 show ap-config radio config

Use this command to display the radio configuration of the specified AP.

show ap-config radioradio-idconfig ap-name

【Parameter Description】

Parameter	Description
radio-id	The id of the radio to be configured, ranging from 1 to 96.
ap-name	Specify the name of the AP to be queried.

【Command Mode】 Privileged mode

【Default Level】 1

【Usage Guide】 -

【Configuration Example】 1: View the configuration information of the specified radio of the specified AP.

```
AC-FS# show ap-config radio 1 config 220em
Admin State.....Enable
Current Tx Power.....Global
Num of BSSIDs.....1
DTIM Period.....1
Beacon Period(milliseconds).....100
Country Code.....CN
Current Channel.....Global
```

Field	Description
Admin State	Radio enabled state.
Current Tx Power	Current transmit power.
Num of BSSIDs	Number of BSSIDs.
DTIM Period	DTIM period.
Beacon Period	Beacon cycle.
Country Code	country code.
Current Channel	use channel.

【Prompt Information】-

【Platform Description】-

5.63 show ap-config radio info

Use this command to display radio information of the specified AP.

show ap-config radio infoap-name

【Parameter Description】

Parameter	Description
ap-name	Specify the name of the AP to be queried.

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】-

【Configuration Example】1: View the radio information of all APs.

```
AC-FS#show ap-config radio info ap-name
Radio ID Radio Type      MU-MIMO    OFDMA      Radio Base MAC  Status
-------- --------------- ---------- ---------- --------------- ------

1        802.11b/g/n Nonsupport          Nonsupport       000c.3067.fbd7
Enable 2        802.11a/n/ac/ax DL          DL/UL       000c.3067.fbd8
```

Field	Description
Radio ID	RF Interface ID.
Radio Type	Working frequency.
MU-MIMO	Multi-user, multiple-input and multiple-output enabling of radio ports, DL is downlink, UL is uplink.
OFDMA	OFDMA enabled status of the RF port, DL is downlink, UL is uplink.
Radio Base MAC	The mac address of the radio port.
Status	RF port status.

【Prompt Information】-

【Platform Description】-

5.64 show ap-config radio radio-id status

Use this command to display details about the radio configuration of the specified AP device.

show ap-config radioradio-idstatus ap-name

【Parameter Description】

Parameter	Description
Radio ID	Radio ID. The range is from 1 to 96.
AP name.	AP device name.

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】 -

【Configuration Example】 1: View the detailed status information of the AP specified radio.

```
AC-FS#  show  ap-config  radio  1  s  220em
Admin State.....Enable
Oper State.....Normal
WTP Radio Statistics
 Last Fail Type.....Statistic Not Supported
 Reset Count.....0
 SW Failure Count.....0
 HW Failure Count.....0
 Other Failure Count.....0
 Unknown Failure Count.....0
 Config Update Count.....0
 Channel Change Count.....2
 Band Change Count.....197
 Current Noise Floor.....---- 102
Assigned WTP BSSID
 WLAN ID.....0
 MAC Address..... 0000.0000.0000
MIC Countermeasures
 WLAN ID.....0
 MAC Address..... 0000.0000.0000
RSNA Error Report From Station
 Client MAC Address..... 0000.0000.0000
 Radio Base MAC..... 0000.0000.0000
```

```
 Radio ID.....1
 WLAN ID.....0
 TKIP ICV Errors.....0
 TKIP Local MIC Failures.....0
 TKIP Remote MIC Failures.....0
 CCMP Replays.....0
 CCMP Decrypt Errors.....0
 TKIP Replays.....0
Statistics
 Tx Fragment Count.....0
 Multicast Tx Count.....0
 Failed Count.....0
 Retry Count.....0
 Multiple Retry Count.....0
 Frame Duplicate Count.....0
 RTS Success Count.....0
 RTS Failure Count.....0
 ACK Failure Count.....0
 Rx Fragment Count.....0
 Multicast RX Count.....0
 FCS Error Count.....0
 Tx Frame Count.....0
 Decryption Errors.....0
 Discarded QoS Fragment Count.....0
 Associated Station Count.....0
 QoS CF Polls Received Count.....0
 QoS CF Polls Unused Count.....0
 QoS CF Polls Unusable Count.....0
Current Tx Power.....100
Current Tx Power Value.....28
Tx Power Level Num.....0
WebAuth online sta Count.....0
DOT1x online sta Count.....0
Security sta Count.....0
WTP Radio Fail Alarm Indication
 Type.....Unknown
 Status.....0
 Pad.....0
WTP Radio Information
Radio Type.....802.11b
WTP Radio Config
```

```
 Short Preamble------------------------------------------ 0
 Number of BSSIDs---------------------------------------- 1
 DTIM Period--------------------------------------------- 0
 Radio Base MAC------------------------------------------ 00d0.f822.33da
 Beacon Period(milliseconds)----------------------------- 100
 Country String------------------------------------------ CNI
Direct Sequence Control
 Current Channel----------------------------------------- 11
 Current CCA--------------------------------------------- 1
 Energy Detect Threshold--------------------------------- 1
MAC Operation
 RTS Threshold------------------------------------------- 2347
 Short Retry--------------------------------------------- 7
 Long Retry---------------------------------------------- 4
 Fragmentation Threshold--------------------------------- 2346
 Tx MSDU Lifetime---------------------------------------- 0
 Rx MSDU Lifetime---------------------------------------- 0
Multi-Domain Capability
 First Channel------------------------------------------- 0
 Number of Channels-------------------------------------- 0
 Max Tx Power Level-------------------------------------- 0
OFDM Control
 Current Channel----------------------------------------- 0
 Band Supported------------------------------------------ 0
 TI Threshold-------------------------------------------- 0
Capability
 Power Default------------------------------------------- 28
 Power Max----------------------------------------------- 28
 Power Min----------------------------------------------- 1
 Power Per Default--------------------------------------- 100
 Power Per Max------------------------------------------- 100
 Power Per Min------------------------------------------- 4
```

Field	Description
WTP Radio Statistics	Radio Statistics.
Assigned WTP BSSID	BSSID information.
MIC Countermeasures	MIC count.
RSNA Error Report From Station	RSNA bug report.
Statistics	Statistics.
WTP Radio Information	Radio Information.

WTP Radio Config	Radio configuration.
Direct Sequence Control	DSC control.
MAC Operation	MAC attribute.
Multi-Domain Capability	Multi-domain capacity.
OFDM Control	OFDM control.
Capability	Power Capacity.

【Prompt Information】-

【Platform Description】-

5.65 show ap-config radio status

Use this command to display the radio list of an AP device.

show ap-config radio statusap-name

【Parameter Description】

Parameter	Description
ap-name	Specify the name of the AP to be queried.

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】-

【Configuration Example】1: Display the radio list of AP.

```
AC-FS# show ap-config radio status 220em
Radio Slot  Radio Type      Sub Band   Admin Status   Oper Status     Regulary Domain      Radio
Base MAC

--------------------------------------------------------------------------------------------
1           802.11b/g/n     -          Enable---------- Supported
00d0.f822.33da
2           802.11a/n       -          Enable---------- Supported
00d0.f822.33db
```

Field	Description

Radio Slot	Radio slot number.
Radio Type	Radio type.
Sub Band	sub bandwidth.
Admin Status	management status.
Oper Status	operating state.
Regulary Domain	rule domain.
Radio Base MAC	Radio MAC address.

【Prompt Information】-

【Platform Description】-

5.66 show ap-config summary radio

Use this command to display all APs on the specified radio.

show ap-config summary radio [radio-id]

【Parameter Description】

Parameter	Description
radio-id	The id of the radio to specify, the range is 1~96.

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】 None

【Configuration Example】 1: View all AP related information under radio 1, including AP name, AP IP address, Radio MAC address, Radio type and number of users.

```
AC-FS#sh ap-config summary radio 1
Ap Name                                  Radio Base MAC  STA NUM  Radio Type   AP IP
---------------------------------------- --------------- -------- ------------ ---------------
AP530-I1.01          0014.4b74.d427          0          802.11b          172.18.57.195          APfloor1
0014.4b6d.e18f  8          802.11b/n/ax 172.18.57.227
```

【Prompt Information】-

【Platform Description】-

5.67 show client details

Use this command to display the information of the specified wireless client.

show client details sta-mac

【Parameter Description】

Parameter	Description
sta-mac	MAC address of the wireless client. The format is H.H.H.

【Command Mode】 Privileged mode

【Default Level】 1

【Usage Guide】 -

【Configuration Example】 1: View 0025.9c9b.aeb5 user statistics.

```
AC-FS# show client details 0025.9c9b.aeb5
The Details of Client 0025.9c9b.aeb5:
    RSSI..... 28
    SNR.....----67
    AID..... 1
    RX Data.....51
    RX Management.....0
    RX Control.....0
    RX Unicast.....25
    RX Multicast.....0
    RX Bytes.....6174
    TX Data.....3
    TX Management.....0
    TX Unicast.....3
    TX Multicast.....0
    TX Bytes.....228
    TX Probe.....0
    TX Assoc.....0
    TX Assoc Fail.....0
    TX Auth.....0
    TX Auth Fail.....0
    TX Deauth.....0
    TX Disassoc.....0
    Packet Load.....51216
```

Field	Description
RSSI	Received signal strength indication.
SNR	signal to noise ratio.
AID	Identity ID.
RX Data	Number of received data frames.
RX Management	Number of received management frames.
RX Control	Receive control frames.
RX Unicast	Number of unicast frames received.
RX Multicast	Number of received multicast frames.
RX Bytes	received bytes.
TX Data	Send data frames.
TX Management	Send management frames.
TX Unicast	Number of unicast frames sent.
TX Multicast	Send multicast frames.
TX Bytes	number of bytes sent.
TX Probe	Send probe frame.
TX Assoc	send association frame.
TX Assoc Fail	Failed to send associated frames.
TX Auth	Number of authentication frames sent.
TX Auth Fail	Number of failures to send authentication frames.
TX Deauth	Number of deauthentication frames sent.
TX Disassoc	Disassociation frames sent.
Packet Load	Throughput.

【Prompt Information】-

【Platform Description】-

5.68 show smart bad radio

Use this command to display the bad radio on AP5280.

show smart bad radio

【Parameter Description】 -

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】 -

【Configuration Example】 The following example displays the bad radio on AP5280.

```
AC#show smart bad radio

Ap-name                 ap-mac                  radio
------------------

AP5280-1        00d0.1234.4565          1,2,3,4,
AP5280-2        00d0.1234.4568          7,8,
```

【Field Description】

Field	Description
Ap name	AP Name.
Ap-mac	AP MAC Address.
radio	Bad Radio ID.

【Prompt Information】-

【Platform Description】 Only the bad card information of AP5280 can be displayed on the AC

5.69 update-key-tsc enable

Use this command to enable the AP device to update key TSC during 802.1x reauthentication.

Use the no form of this command to disable the AP device to update the key TSC.

update-key-tsc enable

no update-key-tsc enable

【Parameter Description】 -

【Default Configuration】 Do not update.

【Command Mode】 AP configuration mode, AP group configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】 The following example enables the AP device to update key TSC during 802.1x reauthentication.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# update-key-tsc enable
```

【Verification】 1: Use the show ap-config running ap-name command to check whether the specified AP is configured to update the encrypted TSC.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.70 show ap-config power-mng poe

Displays the power consumption management of the AM5514 under this AC.

show ap-config power-mng poe

【Parameter Description】 -

【Defaults Level】 1

【Command Mode】 Privilege mode

【Usage Guide】 -

【Configuration Example】 Displays the bad card situation for the AP5280 of this AC.

```
sh ap-config power-mng poe
AP MAC            Power-type    Cur_power    Max_power  Cur_ele   Line_len  Waring
```

Field	Description
AP MAC	AP mac address.
Power-type	Power supply type: Adapter/HPOE power supply.
Cur_power	Current power in mw.
Max_power	Maximum power in mw.
Cur_ele	Current current in ma.
Line_len	Cable length in m.

Warning	Whether the cable impedance exceeds the alarm.

【Prompt Information】 -

【Platform Description】 Power consumption management of AM5514 can only be displayed on AC, not supported by other AP.

5.71 wopt dcca wnable {auto | [0,10]}

Configure the AP pre-ax subfunction dcca auto adjustment or fixed level enabling.

wopt dcca enable {auto | [0,10]}

Configuring the AP pre-ax subfeature dcca does not enable.

no wopt dcca enable

【Parameter Description】 -

【Default Configuration】Not updated.

【Command Mode】 AP configuration mode, AP group configuration mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example】 Enter the configuration mode of AP0001 and configure dcca enables.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# wopt dcca enable auto
```

【Verification】 Using the show ap-config running ap-name command, you can see if the specified AP has configured the dcca.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.72 wopt dtpc enable

Configure the AP pre-ax subfunction dtpc for enabling.

wopt dtpc enable

Configuring the AP pre-ax subfeature dcca does not enable.

No wopt dtpc enable

【Parameter Description】 -

【Default Configuration】 Not updated.

【Command Mode】 AP configuration mode, AP group configuration mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example】 Enter the configuration mode of the AP0001 and configure dtpc enabling.

```
AC-FS(config)# ap-config AP0001
AC-FS(config-ap)# wopt dtpc enable
```

【Verification】 Using the show ap-config running ap-name command, you can see if the specified AP has configured the dtpc.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.73 show wopt dcca

View the dcca configuration.

show wopt dcca

【Parameter Description】 -

【Default Configuration】 Not updated

【Command Mode】 AP configuration mode

【Default Level】 1

【Usage Guide】 -

【Configuration Example】 Enter the console for the AP0001.

```
AC-FS# show wopt dcca
```

【Prompt Information】 Field interpretation：

Field	Interpretation
do ani disable	The disable says that the dcca is on.
ofdm_noise_immunity_level	The current setting level.

【Common Mistake】 -

【Platform Description】 -

5.74 show wopt dtpc

View the dtpc configuration.

show wopt dtpc

【Parameter Description】 -

【Default Configuration】 Not updated

【Command Mode】 AP configuration mode、AP group configuration mode

【Default Level】1

【Usage Guide】 -

【Configuration Example】 Enter the console for the AP0001.

```
AC-FS# show wopt dtpc
```

【Prompt Information】 Field interpretation：

Field	Interpretation
Radio(0) DTPC disable	Whether to make

【Common Mistake】 -

【Platform Description】 -

6 WLAN-WBS-FWD

6.1 central dhcp enable

Configure the local forwarding DHCP message to go AC, the IP address centralized acquisition.

central dhcp enable

Restore the default value with the no command.

no central dhcp enableV

【Parameter Description】 -

【Default Configuration】 In the Default Configuration, the locally forwarded DHCP packets are forwarded locally by the AP, not necessarily through the AC.

【Command Mode】 WLAN configuration mode

【Default Level】 14

【Usage Guide】 To facilitate management of DHCP address pools for wireless users and on, it is recommended to simplify the DHCP topology.

【Configuration Example】 The Tunnel mode configuring the WLAN is local forwarding, but DHCP goes AC, IP address centralized acquisition.

```
AC-FS(config)#wlan-config 100
AC-FS_wlan AC-FS(config-wlan)#tunnel local
AC-FS(config-wlan)#central dhcp enabl
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

6.2 local fw ip

Specifies the user ip address that uses the local forwarding mode.

local fw ip [ip address]

Delete the user ip address with the local forwarding mode.

no local fw ip [ip address]

【Parameter Description】

Parameter	Description
ip address	Accessed user ip address.

【Default Configuration】 No IP specifies local forwarding, forwarding mode with the tunnel configuration.

【Command Mode】 AC-Controller configuration mode

【Default Level】 14

【Usage Guide】 Flexible forwarding function, according to the access of data， automatic identification, using local forwarding or centralized forwarding; It is currently supported to determine which forwarding method is used based on user access to the ip address.

【Configuration Example】 User data configured to access 192.168.1.1 is forwarded locally.

```
AC-FS(config)#ac-controller
AC-FS(config-ac)#local fw ip192.168.1.1
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

6.3 tunnel

WLAN configuration mode in WLAN configuration mode is separate MAC mode or local MAC mode via the tunnel command.

tunnel { 8023 | central | local-auth }

Use the no option for this command to recover to the default mode.

no tunnel

【Parameter Description】

Parameter	Description
8023	AP encapsulates the received wireless data in 802.3 frame format to AC. This mode is the default configuration mode
central	AP forwards wireless data directly locally.
local-auth	In the local authentication forwarding mode, the AP directly forwards the received wireless data locally, and the STA completes the authentication process on the AP side.

【Default Configuration】 By default, the default forwarding mode for the AC is local forwarding.

【Command Mode】 WLAN configuration mode

【Default Level】 14

【Usage Guide】 The local-auth command is only used in RIPT scenarios, which otherwise makes the WLAN unavailable

【Configuration Example】 Example 1：The Tunnel mode that configures the WLAN is local forwarding.

```
AC-FS(config-wlan)#tunnel central
```

Example 2：The Tunnel mode for configuring the WLAN is the 8023 centralized forwarding.

```
AC-FS(config-wlan)#tunnel 8023
```

Example3：The Tunnel mode for restoring the WLAN is in the default mode.

```
AC-FS(config-wlan)#no tunnel
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

6.4 tunnel 8023wlan

Specify a VLAN message under WLAN.

tunnel 8023 wlan [wlan-id] vlan [vlan-id]

Delete a VLAN message under WLAN.

no tunnel 8023 wlan [wlan-id] vlan [vlan-id]

【Parameter Description】

Parameter	Description
wlan-id	To use the id of the centrally forwarded wlan, the wlan must have been created, and the value range is: 1~4094.
vlan-id	To use the id of the vlan to be forwarded centrally, the vlan must have been created, and the value range is: 1~4094.

【Default Configuration】 Packets without any specified VLAN are forwarded centrally, and the forwarding mode is the same as tunnel configuration.

【Command Mode】 AP-group configuration mode

【Default Level】 14

【Usage Guide】 In the WLAN configuration mode, you can specify the forwarding mode of the entire WLAN as local forwarding through tunnel local, However, the tunnel 8023 wlan command can be used to further instruct a certain VLAN packet under the WLAN to be forwarded centrally.

【Configuration Example】Example1: VLAN 2 of wlan 1 is forwarded locally, and packets of other VLANs of wlan 1 are forwarded centrally.

```
AC-FS(config)#wlan-config 1
AC-FS(config-wlan)#tunnel local AC-FS(config-wlan)#exit
AC-FS(config)#ap-group default
AC-FS(config-ap-group)#tunnel 8023 wlan 1 vlan 2
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

6.5 tunnel local wlan

Specifies that packets of a certain VLAN under the WLAN are forwarded locally.

tunnel local wlan [wlan-id] vlan [vlan-id]

Delete a VLAN under the WLAN and forward the packets locally.

no tunnel local wlan [wlan-id] vlan [vlan-id]

【Parameter Description】

Parameter	Description
wlan-id	To use the id of the locally forwarded wlan, the wlan must have been created, and the value range is:1~4094.
vlan-id	To use the id of the locally forwarded vlan, the vlan must have been created, and the value range is:1~4094.

【Default Configuration】 Packets without any specified VLAN are forwarded locally, and the forwarding mode is the same as the tunnel configuration

.

【Command Mode】 AP-group configuration mode

【Default Level】 14

【 Usage Guide 】 In the WLAN configuration mode, the forwarding mode of the entire WLAN can be specified as centralized forwarding through tunnel 8023, however, the tunnel local wlan command can be used to further instruct a certain VLAN packet under the WLAN to be forwarded locally.

【Configuration Example】Exampe1: vlan 2 of wlan 1 is forwarded locally, and packets of other vlans of wlan 1 are forwarded centrally

```
AC-FS(config)#wlan-config 1
AC-FS(config-wlan)#tunnel 8023 AC-FS(config-wlan)#exit
AC-FS(config)#ap-group default
AC-FS(config-ap-group)#tunnel local wlan 1 vlan 2
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

6.6 tunnel-mode

In AC configuration mode, use the tunnel-mode command to configure the AC tunnel mode promiscuous forwarding mode or local forwarding mode.

tunnel-mode { hybrid | local }

Use the default or no option of the command to revert to the default mode.

{ default | no } tunnel-mode

【Parameter Description】

Parameter	Description
hybrid	AC promiscuous forwarding mode, WLAN supports the coexistence of centralized forwarding mode and local forwarding mode , That is, some WLANs are centralized forwarding, and some WLANs are local forwarding.

【Default Configuration】 Promiscuous forwarding mode

【Command Mode】 AC configuration mode

【Default Level】 14

【Usage Guide】 1: The AC forwarding mode switch takes effect only after saving the configuration and restarting the device. Mode switching will not automatically restart, and you need to manually restart the device.

2: Adding or modifying the configuration in the config.text file requires a restart to take effect; deleting the configuration in the config.text file is invalid.

3: The AC forwarding mode configuration is preset in the system, even if it is restarted without writing to save the configuration, it will take effect.

4: Tunnel-mode hybrid is an explicit configuration of the hybrid forwarding mode, which will not be changed after the AC version is upgraded to update the Default Configuration.

5: Switch from hybrid to local. After the device restarts, the centralized forwarding WLAN will automatically switch to local forwarding.

6: Switching from local to hybrid, the WLAN forwarding mode will not be automatically restored or switched after the device restarts.

7: In local mode, the configurations of services that require centralized forwarding remain unchanged but the functions do not take effect. Including but not limited to: broadcast forwarding ratio of DATA-PLANE and configuration of token bucket, WQOS AC-based speed limit, WIDS AC-based or AC SSID-based Layer 2 isolation, application identification and other functions.

8: After the AC forwarding mode is switched, the maximum number of APs and STAs that can be managed will also change accordingly.

9: The AC forwarding mode does not support restoring the Default Configuration by pressing the reset button.

【Configuration Example】 Example 1：Set the Tunnel mode of the AC to local forwarding mode.

```
AC-FS(config-ac)#tunnel-mode local
```

\

Example 2：Configure the tunnel mode of the AC to promiscuous forwarding mode.

```
AC-FS(config-ac)#tunnel-mode hybrid
```

Example 3：Restore the tunnel mode of the AC to the default mode.

```
AC-FS(config-wlan)#default tunnel-mode
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

6.7 vlan-first

The vlan priority function configuration command is configured in the AP configuration mode of the AC device. Configure the vlan priority function to be enabled.

vlan-first global-enable

The user can restore the parameter to the default value with the no option of this command.

no vlan-first global-enable

Configure a priority vlan. When the packets of this priority vlan pass, the vlan priority function takes effect, that is, only the packets of the priority vlan can pass through, and the packets of other vlans are directly discarded. By default, there is no priority vlan.

vlan-first vlan [vian-id]

The user can restore the parameter to the default value with the no option of this command.

no vlan-first vlan [vian-id]

Configure the multicast address of the vlan priority function.

vlan-first ip [sip] [dip]

The user can restore the parameter to the default value with the no option of this command.

no vlan-first ip [sip] [dip]

【Parameter Description】

Parameter	Description
global-enable	The vlan priority function is enabled and disabled by default.
vlan	Configure priority vlan.
[vian-id]	vlan-id: Specifies the preferred VLAN, ranging from 1 to 4094.
ip	Configure the VLAN-preferred multicast address.
[sip]	The source IP address of the multicast address.
[dip]	The destination IP address of the multicast address.

【Default Configuration】 The VLAN priority function is disabled by default; all VLANs are non-priority VLANs by default; there is no multicast address by default.

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 1: Vlan priority function, when the packets of this priority vlan pass, the vlan priority function takes effect, that is, only

the packets of the priority vlan can pass through, and the packets of other vlans are directly discarded。If no packets of the priority VLAN pass through for more than 60S, other non-priority VLAN packets will be released.

2: When the packet of the priority vlan arrives for the first time, a multicast packet is sent, and the multicast address can be configured.

【Configuration Example】

Example 1：Configure the vlan priority function of the specified AP to be enabled.

```
AC-FS(config-ap)#vlan-first global-enable
```

Example 2：Configure the preferred vlan id of the specified AP.

```
AC-FS(config-ac)# vlan-first vlan 100
```

Example 3：Configure the multicast address of the specified AP's vlan priority function.

```
AC-FS(config-wlan)#vlan-first ip 192.168.100.7 224.1.1.1
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

7 DATA-PLANE

7.1 data-plane

Configure the proportion of broadcast forwarding.

data-plane queue-weight unicast-packet-weigh multicast-packet-weight broadcast-packet-weight unknown-multicast-packet-weight unknown-unicast-packet-weight

The user can restore the parameter to the default value with the no option of this command.

no data-plane queue-weight

Configure the update period and multiple of the broadcast forwarding token bucket.

data-plane token token-interval token-base-rate

The user can restore the parameter to the default value with the no option of this command.

no data-plane token

Configuring Broadcast Wireless Forwarding Policy.

data-plane wireless-broadcast { enable | disable }

Users can use the no option of this command to cancel forwarding all broadcasts to the air interface.

no data-plane wireless-broadcast

【Parameter Description】

Parameter	Description
queue-weight	Configure the broadcast forwarding ratio of different types of packets.
wireless-broadcast	Configure whether to forward all broadcast packets to the air interface.
unicast-packet-weight	The proportion of unicast packet forwarding, the range is 1-100, the default value is 16
multicast-packet-weight	The proportion of multicast packets forwarded, the range is 1-50, the default value is 4
broadcast-packet-weight	The proportion of broadcast packets forwarded, the range is 1-50, the default value is 2
unknown-multicast-packet-weight	The forwarding proportion of unknown multicast packets, the range is 1-25, the default value is 8

unknown-unicast-packet-weight	The forwarding proportion of unknown listcast packets, the range is 1-25, the default value is 1
token	Configure the update period and multiple of the broadcast forwarding token bucket
token-interval	The update period of the broadcast forwarding token bucket, the default value is 1, the unit is 10ms
token-base-rate	The multiple of the broadcast forwarding token bucket, the default value of AC is 64, and the default value of AP is 5
token	Configure the update period and multiple of the broadcast forwarding token bucket

【Default Configuration】 By default, the proportion control of broadcast forwarding of different types of packets is enabled; by default,

the forwarding of all broadcast packets to the air interface is not enabled.

【Command Mode】 Global configuration mode.

【Default Level】 15

【Usage Guide】 -

【Configuration Example】 Set the broadcast forwarding weight of different types of packets, and enable forwarding of all broadcast packets to the air interface.

```
AC-FS(config)#data-plane queue-weight 100 50 50 25 25
AC-FS(config)#data-plane token 10 10
AC-FS(config)#data-plane wireless-broadcast enable
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

8 WLOG

8.1 ap-probe ap enable

Configure the AP sniffing hotspot function enables.

ap-probe ap enable

Closed AP sniff hotspot function.

no ap-probe ap enable

【Parameter Description】 -

【Default Configuration】 Default closed

【Command Mode】 AP configuration mode and AP group configuration mode

【Default Level】 15

【Usage Guide】 AP configuration mode and AP group configuration mode

【Configuration Example】 Configure the AP1 to open the sniff hotspot information.

```
AC-FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)# ap-config AP1
AC-FS(config-ap)# ap-probe ap enable
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC device

8.2 ap-probe sta enable

Configuring the AP sniffing terminal function enables .

ap-probe sta enable

Turn off the AP sniff terminal function.

no ap-probe sta enable

【Parameter Description】 -

【Default Configuration】 Default closed.

【Command Mode】 AP configuration and AP group configuration mode

【Default Level】 15

【Usage Guide】 Configure AP on sniff terminal information.

【Configuration Example】 Configure the AP1 to open the sniffing terminal information

```
AC-FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)# ap-config AP1
AC-FS(config-ap)# ap-probe sta enable
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC device

8.3 ap-probe cache-time

Configure the AP sniffing information cache time.

ap-probe cache-time num

Turn off the AP sniff terminal function.

no ap-probe cache-time

【Parameter Description】

Parameter	Description
num	Cache time of sniffing information at the AP end, in seconds, and range from 0 to 3600 seconds.

【Default Configuration】 120 seconds.

【Command Mode】 AP configuration mode and AP group configuration mode

【Default Level】 15

【Usage Guide】 Time to configure the AP cache-sniffing information.

【Configuration Example】 Configure the AP1 cache-sniffing information for 60 seconds

```
AC-FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)# ap-config AP1
AC-FS(config-ap)# ap-probe cache-time 60
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC device

8.4 ap-probe upload-time

Configure the time interval for regular reporting of AP sniffer information

ap-probe upload-time num

Recover the time interval of regular reporting of AP sniffing information.

no ap-probe upload-time

【Parameter Description】

Parameter	Description
num	The time for the AP-side sniffing information to be reported regularly, in seconds, in the range of 1~300 seconds.

【Default Configuration】 5 seconds

【Command Mode】 AP configuration mode and AP group configuration mode

【Default Level】 15

【Usage Guide】 Configure the regular reporting time for the AP sniffing information.

【Configuration Example】 Configure the AP1 sniffing information to report regularly every 6 seconds

```
AC-FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)# ap-config AP1
AC-FS(config-ap)# ap-probe upload-time 6
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

8.5 ap-probe limit

Configure the maximum number of AP-terminal cache sniffing information

ap-probe limit num

Restore the maximum number of AP-terminal cache-sniffing information.

no ap-probe limit

【Parameter Description】

Parameter	Description
num	The number of AP-end sniffing information that can be cached

【Default Configuration】 100

【Command Mode】 AP configuration mode and AP group configuration mode

【Default Level】 15

【Usage Guide】 Configure the maximum number of AP-terminal cache sniffing information.

【Configuration Example】 Configure the AP1 with up to 200 information on cache sniffing.

【Verification】 -

【Prompt Information】-

【Common Mistake】 -

【Platform Description】 AC device

8.6 show wlan diag ap

Use this command to display AP records on an AC.

show wlan diag ap [ap-macAP_MAC] [number NUMBER]

【Parameter Description】

Parameter	Description
AP_MAC	Specifies the MAC address of an AP to be displayed.
NUMBER	Specifies the maximum number of records to be displayed.

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】 None

【Configuration Example】1: Display AP record information:

```
AC-FS# show wlan diag ap ap-mac 00d0.f822.33b0 number 10

ap_record: AC-FSAP[00d0.f822.33b0/1.1.1.2],down/up:2

IP Address:1.1.1.2
2012-05-28 09:30:00  [TIMER]      AP UP Time: 00:00:18:54
```

```
Wired port five in rate/out rate stat:612kbits/sec(in) 1208kbits/sec(out)
   Unicast:    84595   bytes(in) 86625   bytes(out)
   Multicast:  7       bytes(in) 4       bytes(out)
   Broadcast:  2145    bytes(in) 117     bytes(out)
   Error Frame:0       bytes(in) 0       bytes(out)
Radio    channel power       Active STA WEB_Auth   DOT1X       Rssi     ErrorPkt   RetryPkt

1        11      100        2          1          0          0        0          0
2        157     100        0          0          0          0        0          0

IP Address:1.1.1.2
2012-05-28 09:49:18  [CW-DOWN]    AP UP Time: 00:00:38:12
Wired port five in rate/out rate stat:187kbits/sec(in) 905kbits/sec(out)
   Unicast:    84789   bytes(in) 86810   bytes(out)
   Multicast:  7       bytes(in) 5       bytes(out)
   Broadcast:  2148    bytes(in) 133     bytes(out)
   Error Frame:0       bytes(in) 0       bytes(out)
Radio    channel power       Active STA WEB_Auth   DOT1X       Rssi     ErrorPkt   RetryCnt

1        11      100        2          1          0          0        0          0
2        157     100        0          0          0          0        0          0
CAPWAP DOWN REASON:echo expired
```

Field	Description
ap_record	Specifies AP records.
IP Address	Specifies the IP address of an AP whose information is collected.
TIMER	Specifies information collected by a timer.
CW-DOWN	Specifies information collected when a CAPWAP connection is interrupted.
Wired port five in rate/out rate stat	Specifies the input or output rate on a wired port for the recent five minutes.
Unicast	Specifies statistics about unicast packets on a wired port.
Multicast	Specifies statistics about multicast packets on a wired port.

Broadcast	Specifies statistics about broadcast packets on a wired port.
Error Frame	Specifies statistics about incorrect frames on a wired port.
Radio	Specifies a radio ID.
channel	Specifies the working channel of the radio.
power	Specifies the emission frequency of the radio.
Active STA	Specifies the number of STAs associated with the radio.
WEB_AUTH	Specifies the number of STAs associated with the radio and get online through the web interface.
DOT1X	Specifies the number of STAs associated with the radio and get online through 802.1X authentication.
ErrorPkt	Specifies the number of incorrect frames received by the radio.
RetryCnt	Specifies the number of times that packets from the radio are retransmitted.
CAPWAP DOWN REASON	Specifies the reason for CAPWAP disconnection. This item is displayed only when CW_DOWN is set.

【Prompt Information】 -

【Platform Description】 AC

8.7 show wlan diag network

Use this command to display the record information about the entire network.

show wlan diag network

【Parameter Description】 -

【Command Mode】 Privileged mode

【Default Level】 1

【Usage Guide】 None

【Configuration Example】 1: Display the current network overview record information:

```
AC-FS# show wlan diag network
    Time: 2012-05-28 09:10:00
    AC uptime: 1 h
    Online  AP: 1
    Online AP Version:
        PID[AP220-E]:hwver[2.00] AP Number:1
    Offline AP:7
    ssid                            Active STA WEB Auth   Dot1x      Free STA
    ------------------------------- ---------- ---------- ---------- ----------
    1T17-wlog-test1                 0          0          0          0
    1T17-wlog-test2                 0          0          0
```

Field	Description
Time	Specifies the time for collecting a record.
AC Running Time	Specifies the running time of an AC connection.
Current Online Number of AP	Specifies the number of online APs.
Online AP Version	Specifies the version of online APs.
Offline Number of AP	Specifies the number of pre-configured but offline APs.
ssid	Specifies the SSID of a WLAN.
Active STA	Specifies the total number of active STAs.
WEB Auth	Specifies the number of STAs that get online through web authentication.
Dot1x	Specifies the number of STAs that get online through 802.1x authentication.
Free STA	Specifies the number of STAs free of authentication.

【Prompt Information】-

【Platform Description】 AC

8.8 show wlan diag sta

Use the following command to display STA statistics on an AC:

show wlan diag sta [sta-mac STA_MAC] [ip-range IP_PREFIX] [action ACTION[result RESULT]] [number NUMBER]

Use the following command to display STA statistics on an AP:

show wlan diag sta [sta-mac STA_MAC] [number NUMBER]

【Parameter Description】

Parameter	Description
STA_MAC	Specifies the MAC address of an STA.
IP_PREFIX	Specifies the range of IP addresses for the STA, which is limited by an IP prefix.
ACTION	Specifies the type of STA action records.
RESULT	Specifies the result of STA action records.
NUMBER	Specifies the maximum number of records to be displayed.

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】 None

【Configuration Example】1: View terminal information on AC:

```
AC-FS# show wlan diag sta
sta_record: c83a.35c6.0c72
[STA-DOWN]   STA UP Time: 2018-04-19 22:06:05      STA DOWN Time: 2018-04-19 22:11:17
Time      IP Address      RSSI/Link        Rate        DEV        ID/AP        MAC/SSID/Radio
Action               Result Reason

-------------------------------------------------------------------------------------------
09:59:28 0.0.0.0         0/0.0M          1/00d0.f822.33b0/lxh-ssid/1                    STA
UP BY APMG       SUCCESS
10:12:07 192.168.248.2----- 88/13.0M       1/00d0.f822.33b0/lxh-ssid/1                   STA
DOWN BY APMG             AP circular AC user is offline
```

```
tx/rxrate     1, 2    5.5, 11 6, 9    12, 18  24, 36  48, 54 ----------------
------------ ------- ------- ------- ------- ------- ------- ------- -------
txratepercent: 16      0       0       7       50      27      0       0
rxratepercent: 57      3       0       5       13      22      0       0
```

Field	Description
sta_record	Specifies STA records.
TIME	Specifies the time when STA records are collected.
IP Address	Specifies the IP address of an STA whose statistics are collected.
Rssi	Specifies signal strength.
Link Rate	Specifies a connection rate.
AP MAC	Specifies the MAC address of an AP associated with the STA.
SSID	Specifies the SSID of the WLAN associated with the STA.
RADIO	Specifies the ID of the radio associated with the STA.
Action	Specifies the type of STA action records.
Result	Specifies the result of STA action records.
Reason	Specifies the reason for STA action records.

【Prompt Information】 -

【Platform Description】 AC, fat AP

8.9 wlan diag enable

Configure the WLOG function to enable.

wlan diag enable

Turn off the WLOG function.

no wlan diag enable

【Parameter Description】 -

【Default Configuration】 The WLOG function on AC and AP devices is disabled by default.

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】 Configuring the WLOG function enables pre-allocation of memory. If there is not enough memory, the WLOG function will fail to enable. When the WLOG function is turned off, all information memory and pre-allocated memory will be released.

【Configuration Example】 The following example enables and disables the WLOG function:

```
AC-FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)#wlan diag enable
AC-FS(config)#no wlan diag enable
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 AC, fat AP

8.10 web-server enable api-path assoc-sta url

Configure the connected Elog server address

web-server enable api-path assoc-sta url url

Delete a connected Elog server address.

no web-server enable api-path assoc-sta url url

Delete all connected Elog server addresses.

no web-server enable api-path assoc-sta url

【Parameter Description】

Parameter	Description
url	Sets the Elog server URL

【Default Configuration】 By default, it is not connected to the Elog server.

【Command Mode】 Global configuration mode

【Default Level】15

【Usage Guide】 To be able to send data smoothly, WLOG must be enabled, and if local forwarding is used, configure ip dhcp snooping in global configuration mode to ensure that the terminal can obtain the IP address. A maximum of 8 Elog server addresses can be configured for docking.

【Configuration Example】 1: Configuration and deletion of STA online and offline information to an Elog server address.

```
AC-FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)#web-server enable api-path assoc-sta url
http://172.18.155.14:8080/elog/service/dc/updateStaAC-FS(config)#no web-server enable api-path
assoc-sta url http://172.18.155.14:8080/elog/service/dc/updateSta
```

2: Configuration and deletion of STA online and offline information to connect to multiple Elog server addresses.

```
AC-FS# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AC-FS(config)#web-server enable api-path assoc-sta url
http://172.18.155.14:8080/elog/service/dc/updateSta
AC-FS(config)#web-server enable api-path assoc-sta url
http://172.18.155.15:8080/elog/service/dc/updateSta
AC-FS(config)#no web-server enable api-path assoc-sta url
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

8.11 web-server enable api-path probe-ap url

Configure the Elog server address for sniffing hotspot information docking.

web-server enable api-path probe-ap url url

Remove an Elog server address for sniffing the hot spot information docking.

no web-server enable api-path probe-ap url url

Remove all of the Elog server addresses for sniffing hotspot information docking.

no web-server enable api-path probe-ap url

【Parameter Description】

Parameter	Description
url	The full address of the Elog server

【Default Configuration】 Default does not connect with the Elog server.

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】 Maximum configurable docking of 8 ELOG server addresses.

【Configuration Example】 1. Hot-spot sniffing information connects with the configuration and deletion of an ELOG server.

```
AC-FS# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AC-FS(config)# web-server enable api-path probe-ap url
http://172.21.155.131:8080/elog/service/dc/updateAcCapturedSsid
AC-FS(config)# no web-server enable api-path probe-ap url
http://172.21.155.131:8080/elog/service/dc/updateAcCapturedSsid
```

2: The configuration and deletion of hot sniffing information to multiple ELOG servers.

```
AC-FS# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AC-FS(config)# web-server enable api-path probe-ap url
http://172.21.155.131:8080/elog/service/dc/updateAcCapturedSsid
AC-FS(config)# web-server enable api-path probe-ap url
http://172.21.155.132:8080/elog/service/dc/updateAcCapturedSsid
AC-FS(config)# no web-server enable api-path probe-ap url
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

8.12 web-server enable api-path probe-sta url

Configure the Elog server address for sniffing the STA information docking.

web-server enable api-path probe-sta url url

Remove an Elog server address for sniffing for the STA information docking.

no web-server enable api-path probe-sta url url

Remove the Elog server address for the full sniffing STA information docking.

no web-server enable api-path probe-sta url

【Parameter Description】

Parameter	Description
url	The full address of the Elog server

【Default Configuration】 Default does not connect with the Elog server.

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】 Maximum configurable docking of 8 ELOG servers.

【Configuration Example】 1: The STA sniffing information connects with the configuration and deletion of an ELOG server.

```
AC-FS# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AC-FS(config)# web-server enable api-path probe-sta url
http://172.21.155.131:8080/elog/service/dc/updateAcCapturedSta
AC-FS(config)# no web-server enable api-path probe-sta url
http://172.21.155.131:8080/elog/service/dc/updateAcCapturedSta
```

2: STA sniffing information connects the configuration and deletion of multiple ELOG servers.

```
AC-FS# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AC-FS(config)# web-server enable api-path probe-sta url
http://172.21.155.131:8080/elog/service/dc/updateAcCapturedSta
AC-FS(config)# web-server enable api-path probe-sta url
http://172.21.155.132:8080/elog/service/dc/updateAcCapturedSta
AC-FS(config)# no web-server enable api-path probe-sta url
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

8.13 web-server enable api-path probe-sta syslog

Configure the sniffing STA information print syslog.

web-server enable api-path probe-sta syslog

Remove the sniff STA information to print the syslog.

no web-server enable api-path probe-sta syslog

【Parameter Description】 -

【Default Configuration】 Default to close the sniff STA information print syslog

【Command Mode】 Global configuration mode

【Default Level】15

【Usage Guide】 This command is mutually exclusive with the sniffing hotspot / STA docking ELOG server command, allowing you to configure the command or the sniffing hotspot / STA docking ELOG server command.

【Configuration Example】 STA sniffing information print SYSLOG configuration and deletion

```
AC-FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)# web-server enable api-path probe-sta syslog
AC-FS(config)# no web-server enable api-path probe-sta syslog
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

8.14 web-server enable api-path auth-sta url

Configure the BCR server address for the docking.

web-server enable api-path auth-sta url url

Remove the docked BCR server address.

no web-server enable api-path auth-sta url

【Parameter Description】

Parameter	Description
url	The address of the BCR server

【Default Configuration】 Do not connect with the BCR server by default.

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】 In global configuration mode, WLOG is enabled first, and then the network supervisor docking server address is configured (the website information requires http and proline / Msgbehind the website), url only needs to be configured to? Before the number.

【Configuration Example】 1: Configuration and deletion of the url for docking with the BCR .

```
AC-FS# configure terminal  Dnter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)#wlan diag enable
AC-FS(config)#web-server enable api-path auth-sta url http://10.18.78.149:19900/pronline/Msg
```

2: Removal of the url for docking with the BCR

```
AC-FS(config)#no web-server enable api-path auth-sta url
```

【Verification】 show running-config displays the configured url information.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

8.15 web-server enable api-path auth-sta type

Configure the BCR network monitoring equipment certification type

web-server enable api-path auth-sta type url

The recovery BCR Network Monitor device authentication type is the default value

no web-server enable api-path auth-sta type

【Parameter Description】

Parameter	Description
type	BCR network supervisor certification type value

【Default Configuration】 Default type 1020004.

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】 In global configuration mode, first enable WLOG, and then use the command to configure the authentication type for the BCR.

【Configuration Example】 1: Configure the docking BCR authentication type

```
AC-FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
 AC-FS(config)#wlan diag enable
AC-FS(config)#web-server enable api-path auth-sta type 1020002
```

2: Remove the docking BCR authentication type configuration

```
AC-FS(config)#no web-server enable api-path auth-sta type
```

【Verification】 show running-config displays the configured type information

Delete the configuration information with no restores the default value and show run does not display

【Prompt Information】 -

【Common Mistake】 -

9. ROAM

9.1 keepalive-count

Configure the maximum number of live message sent.

keepalive-count counts

Delete the maximum number of times of configuration.

no keepalive-count

Restore the Default Configuration.

default keepalive-count

【Parameter Description】

Parameter	Description
counts	Maximum number of live message sent.

【Default Configuration】 Four default 4 default after creating a roaming group.

【Command Mode】 Roaming group configuration mode

【Default Level】 15

【Usage Guide】 If the environment is very unstable, you can increase the maximum number of live messages, which can avoid breaking off the roaming tunnel due to a temporary loss of bags

【Configuration Example】 1: After configure a roaming group, configure the maximum number of live message sent 5.

```
AC-FS(config)#mobility-group mgroup_name
AC-FS(config-mobility)# keepalive-count 5
```

【Verification】 Use the show mobility summary command so that you want to view the configuration values.

【Prompt Information】 1: An error is prompted if the value entered is incorrect.

```
Invalid input detected at '^' marker
```

2: If you configure this command, the new configuration overrides the original configuration (No Prompt Information).

【Common Mistake】 -

【Platform Description】 -

9.2 keepalive-interval

Configure the time interval during which the live protection message is sent.

keepalive- interval seconds

Restore the Default Configuration.

no keepalive- interval

Restore the Default Configuration.

default keepalive- interval

【Parameter Description】

Parameter	Description
seconds	Time interval when the live message is sent

【Default Configuration】 Default is 10 seconds after creating a roaming group.

【Command Mode】 Roaming group configuration mode

【Default Level】 15

【Usage Guide】 If you have too many roaming members in your environment, you can extend the time interval and reduce the number of messages sent.

【Configuration Example】1: After a roaming group is configured, configure the live message delivery interval for 20 seconds.

```
AC-FS(config)#mobility-group mgroup_name
AC-FS(config-mobility)# keepalive-interval 20
```

【Verification】 Use the show mobility summary command so that you want to view the configuration values.

【Prompt Information】 1: An error is prompted if the value entered is incorrect.

Invalid input detected at '^' marker

2: If you configure this command, the new configuration overrides the original configuration. (No Prompt Information)

【Common Mistake】 -

【Platform Description】 -

9.3 list

Configure a roaming list member

list { ip-address }

Delete the specified list members.

no list { ip-address.

Delete the specified member by restoring the default

default list { ip-address }

【Parameter Description】

Parameter	Description
ip-address	The IPV4 address of the member AC

【Default Configuration】 No list members.

【Command Mode】 Roaming group configuration mode

【Default Level】 15

【Usage Guide】 the roaming group member location is not enough, you can be supplemented with the roaming list members to realize roaming

【Configuration Example】 After configure a roaming group, add two roaming member lists.

```
AC-FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)#mobility-group mgroup_name
AC-FS(config-mobility)# list 192.168.2.1
AC-FS(config-mobility)# list 192.168.2.2
```

【Verification】 Use the **show mobility summary** command so that you want to view the configuration values.

【Prompt Information】 1: An error is prompted if the value entered is incorrect.

```
Invalid input detected at '^' marker
```

2: An error is prompted if the IP address you entered is illegal：

```
Invalid ip address of member/list, please check your input.
```

3: If you configure this command, the prompt already exists.

```
member/list has existing.
```

4: An error is prompted if the repeated address is the AC itself

```
can not config AC itself as a member/list..
```

【Common Mistake】 -

9.4 member

Configure the roaming group members

member { ip-address }

Delete the specified roaming group member.

no member { ip-address }

Removing the default removes the specified roaming group member.

default member { ip-address }

【Parameter Description】

Parameter	Description

ip-address	The IPV4 address of the member AC.

【Default Configuration】 No list members

【Command Mode】 Roaming group configuration mode

【Default Level】 15

【Usage Guide】 When the roaming group member location is not enough, you can be supplemented with the roaming list members to realize roaming.

【Configuration Example】 After configure a roaming group, add two roaming member lists.

```
AC-FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)#mobility-group mgroup_name
AC-FS(config-mobility)# member 192.168.1.2
AC-FS(config-mobility)# member 192.168.1.3
```

【Verification】 Use the show mobility summary command so that you want to view the configuration values.

【Prompt Information】 1: An error is prompted if the value entered is incorrect.

```
Invalid input detected at '^' marker
```

2: Error is prompted if the entered IP address is illegal:

```
Invalid ip address of member/list, please check your input.
```

3: If you configure this command, the prompt already exists.

```
member/list has been existing.
```

4: An error is prompted if the repeated address is the AC itself.

```
can not config AC itself as a member/list.
```

【Common Mistake】 1: Configured members cannot communicate.

2: The roaming group names configured at both ends are inconsistent.

3: One end does not configure the other party as a member.

【Platform Description】 -

9.5 mobility-fast

Turn on the active information exchange.

mobility-fast

Turn off the active information exchange.

no mobility-fast

Turn off the active information exchange.

default mobility-fast

【Parameter Description】 -

【Default Configuration】 The active information exchange function is turned off.

【Command Mode】 Roaming group configuration mode

【Default Level】 15

【Usage Guide】 When roaming STA is less, opening active information exchange to reduce roaming time-consuming. If too many roaming STA is turned on, opening active information exchange will increase the burden of AC

【Configuration Example】 1: After configure a roaming group, add two roaming member lists.

```
AC-FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)#mobility-group mgroup_name
AC-FS(config-mobility)# mobility-fast
```

【Verification】 Use the show mobility summary command so that you want to view the configuration values.

【Prompt Information】 If you configure the command, the new overrides the old. (No Prompt Information)

【Common Mistake】 -

【Platform Description】 -

9.6 mobility-group

Create a roaming group

mobility-group group-name

Delete a roaming group

no mobility-group group-name

Delete a roaming group

default mobility-group group-name

【Parameter Description】

Parameter	Description
group-name	Roaming group name, with a maximum length of 63

【Default Configuration】 No roaming group.

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】 When AC inter roaming is required, you must create a roaming group.

【Configuration Example】 Configure a roaming group.

```
AC-FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)#mobility-group mgroup_name
```

【Verification】 Use the show mobility summary command, so that you can view the configuration results.

【Prompt Information】 1: An error is prompted if the roaming group name exceeds 63.

```
Group name is too long, must be shorter than 63.
```

2: If the settings repeat, enter the roaming group configuration mode（No Prompt Information）.

【Common Mistake】 1: No PING can pass between the roaming AC.

2: An AC does not configure a roaming group or a member.

3: The roaming group names were not consistent for the different AC.

【Platform Description】 -

9.7 mti-ping

Test whether the roaming members are connected

mti-ping { ip-address }

【Parameter Description】

Parameter	Description
ip-address	The IP address of the member AC

【Default Configuration】 -

【Command Mode】 Roaming group configuration mode

【Default Level】 15

【Usage Guide】 When both the roaming group and the roaming members are established and are not connected, you can view the tunnel to locate the problem by mti-ping.

【Configuration Example】 Perform a single roaming member connectivity test.

```
AC-FS(config)#mobility-group my_group_name
AC-FS(config-mobility)#mti-ping 192.168.1.2
Sending 4, MTI packet to  192.168.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (4/4)
```

【Verification】 View the execution results directly.

【Prompt Information】 1：An error is prompted if the value entered is incorrect.

```
Invalid input detected at '^' marker
```

2：If the test results are not work, there will be hints.

```
Sending 4, MTI packet to  192.168.1.1, timeout is 2 seconds:
....
Success rate is 0 percent (0/4)
```

【Common Mistake】 1: This command is not a ping command, and a successful ping does not mean that mti-ping can be communicated.

2: The object of mti-ping must be a member of the roaming group. If it is not a member of the group, mti-ping will fail even if the ping can pass.

【Platform Description】 -

9.8 roaming central-unroam

Configure local forwarding to turn off roaming, and users will communicate with the VLAN of the new AP map.

roaming local-unroam

Configure local forwarding to open roaming

no roaming local-unroam

Configure local forwarding to open roaming.

default roaming local-unroam

【Parameter Description】 -

【Default Configuration】 The locally forwarded user will still communicate with the roaming VLAN after roaming

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】None

【Configuration Example】 Configure local forwarding to turn off roaming

```
AC-FS(config)# roaming local-unroam
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 Some terminals will not reinitiate the DHCP process after roaming, and directly use the pre-roaming IP to

communicate for communication, so STA IP can be forwarded in the VLAN before and after roaming, and requires whole network deployment, such as deployment with super vlan.

【Platform Description】 All of the wireless AC's

9.9 roaming local-unroam

Configure local forwarding to disable roaming, users will use the VLAN mapped by the new AP for communication after roaming.

roaming local-unroam

Configure local forwarding to enable roaming.

no roaming local-unroam

Configure local forwarding to enable roaming.

default roaming local-unroam

【Parameter Description】–

【Default Configuration】 After roaming, the locally forwarded users still use the VLAN before roaming for communication.

【Command Mode】 Global configuration mode

【Default Level】15

【Usage Guide】 None

【Configuration Example】 1: Configure local forwarding to disable roaming.

```
AC-FS(config)# roaming local-unroam
```

【Verification】-

【Prompt Information】-

【Common Mistake】 1. Some terminals will not re-initiate the DHCP process after roaming, and directly use the IP before roaming for communication. Therefore, the STA's IP needs to be forwarded in the VLAN before and after roaming, and the entire network needs to be deployed. For example Deploy with super vlan.

【Platform Description】 All wireless AC

9.10 roaming logging rate-limit

With the roaming logging rate-limit, you can configure the maximum output number of roaming syslog bars per second.

roaming logging rate-limit limit-num

Restore the Default Configuration.

no roaming logging rate-limit

Restore Default Configuration.

default roaming logging rate-limit

【Parameter Description】

Parameter	Description
limit-num	For the syslog of STA roaming, the maximum number of entries per second. Value range: 1-10000.

【Default Configuration】 Up to 5 syslog s per output per second.

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】 -

【Configuration Example】 The maximum number of bars per second for the configuration to output the syslog is 100.

```
AC-FS(config)# roaming logging rate-limit 100
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

9.11 roaming support wlan

With roaming support wlan you can configure to prohibit or allow user roaming within the wlan.

no roaming support wlan *wlan-id*

Restore the Default Configuration.

roaming support wlan *wlan-id*

Restore the Default Configuration.

default roaming support wlan wlan-id

【Parameter Description】

Parameter	Description
wlan-id	For the wlan of the STA roaming, take the value range: 1-4094

【Default Configuration】 The STA within the wlan supports roaming.

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】 N/A

【Configuration Example】 Configure the STA users within the wlan 1 against roaming.

```
AC-FS(config)# no roaming support wlan 1
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

9.12 show mobility statistics

View the roaming statistics.

show mobility statistics

【Parameter Description】 -

【Command Mode】 Power mode, global mode, roaming group configuration mode

【Default Level】 15

【Usage Guide】 Use this command to view the statistics of all the roaming behavior on the AC.

【Configuration Example】 View the statistics for all roaming behavior on this AC.

```
AC-FS#show mobility statistics
Global Mobility Statistics
Rx Errors.....0
Tx Errors.....0
Response Retransmitted.....0
Handoff Requests Received.....0
Handoff End Requests Received.....0
State Transitions Disallowed.....0
Resource Unavailable.....0
```

```
Mobility Initiator Statistics
Handoff Request Sent.....0
Handoff Reply Received.....0
Handoff As Local Received.....0
Handoff As Foreign Received.....0
Anchor Request Sent.....0
Anchor Deny Received.....0
Anchor Grant Received.....0
Anchor Transfer Received.....0

Mobility Responder Statistic
Handoff Request Ignored.....0
Handoff Request Dropped.....0
Handoff Request Deny.....0
Client Handoff As Local.....0
Client Handoff As Foreign.....0
Anchor Request Received.....0
Anchor Requests Deny.....0
Anchor Requests Granted.....0
Anchor Transfered.....0
```

【Field interpretation】

Field	Interpretation
Global Mobility Statistics	Global roaming statistics.
Rx Errors	Number of times the error packets were received.
Tx Errors	Number of contracting errors.
Response Retransmitted	The number of response repasses.
Handoff Requests Received	Number of requests received.
Handoff End Requests Received	Number of times requests.
State Transitions Disallowed	The number of times that the state transitions were rejected.
Resource Unavailable	Number of times that the resource is unavailable.
Mobility Initiator Statistics	Statistics are used as the roaming initiator.
Handoff Request Sent	The number of requests sent.
Handoff Reply Received	Number of reply requests received.
Handoff As Local Received	The number of local requests.
Handoff As Foreign Received	Number of foreign requests.
Anchor Request Sent	Number of Anchor requests sent.

Anchor Deny Received	Number of Anchor rejections.
Anchor Grant Received	Number of times the Anchor allows.
Anchor Transfer Received	The number of Anchor transfers.
Mobility Responder Statistic	As the statistics of the roaming receiver.
Handoff Request Ignored	Number of requests ignored.
Handoff Request Dropped	Number of requests lost.
Handoff Request Deny	Number of requests rejected.
Client Handoff As Local	Number of local customer requests.
Client Handoff As Foreign	Number of requests.
Anchor Request Received	Number of times the Anchor requests were received.
Anchor Requests Deny	Number of times the Anchor requests were rejected.
Anchor Requests Granted	Number of times the Anchor requests are allowed.
Anchor Transfered	The number of Anchor transfers.

【Prompt Information】 -

【Platform Description】 -

9.13 show mobility status

View the status information for the specified roaming group.

show mobility status group-name

【Parameter Description】

Parameter	Description
group-name	Roaming group name.

【Command Mode】 Privilege mode, global mode, roaming group configuration mode

【Default Level】 15

【Usage Guide】 Use this command to view the statistics of all the roaming behavior on the AC.

【Configuration Example】 View the statistics for all roaming behavior on this AC.

```
AC-FS# show mobility status mgroup_name
Mobility Group mgroup_name
Mobility Keepalive Interval.....10
Mobility Keepalive Count.....3
Mobility Group Status.....normal

Mobility Members:
IP Address          Client/Server Data Tunnel Ctrl Tunnel
192.168.1.2         Client            OK              OK Mobility
List Members:
IP Address          Client/Server   Data Tunnel    Ctrl Tunnel
```

【Field interpretation】

Field	Interpretation
Mobility Group	Roaming group name.
Mobility Keepalive Interval	Time interval at which the roaming group live message is sent.
Mobility Keepalive Count	Maximum number of roaming group message messages.
Mobility Group Status	The status of the roaming group.
Mobility Members	A member of the roaming group.
IP Address	Member, IP, Address.
Client/Server	The transmitter of the tunnel establishment is still the receiver.
Data Tunnel	Whether the data channel is established.
Ctrl Tunnel	Control whether the channel is established.
Mobility List Members	Wandering group list members.

【Prompt Information】 -

【Platform Description】 -

9.14 show mobility summary

View all roaming group status information.

show mobility summary

【Parameter Description】 -

【Command Mode】 Privilege mode, global mode, roaming group configuration mode

【Default Level】 15

【Usage Guide】 Use this command to view the statistics of all the roaming behavior on the AC.

【Configuration Example】 View the statistics for all roaming behavior on this AC.

```
AC-FS# show mobility summary
Mobility Group mgroup_name
Mobility Keepalive Interval.....10
Mobility Keepalive Count.....3
Mobility Group Status.....normal
Mobility Members:
IP Address          Client/Server Data Tunnel Ctrl Tunnel
192.168.1.2         Client            OK              OK
```

```
Mobility List Members:
IP Address          Client/Server   Data Tunnel    Ctrl Tunnel

Mobility Group mgroup_name2
Mobility Keepalive Interval.....10
Mobility Keepalive Count.....3
Mobility Group Status.....normal
Mobility Members:
IP Address          Client/Server  Data Tunnel   Ctrl Tunnel
Mobility List Members:
IP Address          Client/Server   Data Tunnel    Ctrl Tunnel
```

Field interpretation:

Here is lists all roaming groups, exactly with a single show mobility status content.

【Prompt Information】 -

【Platform Description】 -

9.15 show mobility user

View the roaming user information.

show mobility user [mac]

【Parameter Description】

Parameter	Description
mac	Specifies the MAC address of the STA

【Command Mode】 Privilege mode, global mode, roaming group configuration mode

【Default Level】 15

【Usage Guide】 Use this command to view all of the roaming user information on the AC.

【Configuration Example】 1. View the information for the specified roaming STA neg.

```
AC-FS# show mobility user 00:26:0c:ef:6d:12 MAC:
0026.0cef.6d12
IPv4-Address: 20.0.0.2 WLAN: 1
TYPE: LRC
ROC-AC: N/A
ROC-AP: 004c.0cef.6d11
```

```
ROC-VLAN: 2
RIC-AC: N/A
RIC-AP:
004c.0cef.6d12
RIC-VLAN: 3
```

【Field interpretation】

Field	Interpretation:
MAC	The MAC address of the STA.
IPv4-Address	The IPv4 address of the STA..
WLAN	The ID of the WLAN
TYPE	Roaming type.
ROC-AC	Roaming in AC.
ROC-AP	Roaming in AP.
ROC-VLAN	Roaming in VLAN.
RIC-AC	Roaming out AC
RIC-AP	Roaming out AP.
RIC-VLAN	Roaming out VLAN.
ROC-VLAN	Roaming in VLAN.

2: View all roaming STA information.

```
AC-FS# show mobility user
STA-MAC    IPv4-Address IPv6-Address    WLAN TYPE ROC-VLAN RIC-VLAN
_____ _____ _____ ____ ____ _____ _____
0026.0cef.6d12  20.0.0.2    N/A          1   LRC  2     2
0040.0cef.6d33.....20.0.0.5   N/A          2   RIC  3     3
0040.0cef.6d44 20.0.0.6    N/A     3   ROC  2     4
```

【Field interpretation】

Field	Interpretation
STA-MAC	The MAC address of the STA.
IPv4-Address	The IPv4 address of the STA.
WLAN	The ID of the WLAN.
TYPE	Roaming type.
ROC-VLAN	the VLAN before roaming.
RIC-VLAN	the VLAN after roaming.

【Prompt Information】 -

【Platform Description】 -

9.16 show mobility user roam-track

View the roaming track information for the roaming user.

show mobility user roam-track mac

【Parameter Description】

Parameter	Description
mac	Specify the user MAC to view.

【Command Mode】 Privilege mode, global mode, roaming group configuration mode

【Default Level】 15

【Usage Guide】 Use this command to view the roaming track information for the specified user on the AC.

【Configuration Example】 View the roaming track information for the d85d.4c7e.d4c0 on this AC.

```
AC-FS#show mobility user roam-track d85d.4c7e.d4c0

ID        AC-Info           AP-Info        Online-time(d:h:m:s)

1---------LOCAL-           001a.a94e.d41E/1  0:00:00:12
2       192.168.170.12    001a.a94e.d40d/1  0:00:00:24
3---------LOCAL-           001a.a94e.d42A/1  0:00:00:24
```

【Field interpretation】

Field	Interpretation
ID	The number of the roaming sequence.
AC-Info	Information about the affiliated AC.
AP-Info	Information about the associated AP.
Online-time(d:h:m:s)	duration of association.

【Prompt Information】 -

【Platform Description】 -

10 Interface Management

10.1 ap-subif

The wireless AP device will create a sub-interface of the WAN port by default to implement STA data traffic with TAG forwarding. In wireless routing mode (the AP can assign addresses to users), the user's gateway is on the AP, and the corresponding packets do not need to be forwarded with TAG. You can use this command to delete the AP's WAN port sub-interface and avoid the user's gateway address. The same causes address conflict.

ap-subif enable

Unconfigure.

no ap-subif enable

【Parameter Description】-

【Default Configuration】-

【Command Mode】 AP configuration mode/all AP configuration mode

【Default Level】 15

【Usage Guide】 When the AP obtains the address through PPPoE dial-up, the sub-interface of the WAN port of the AP will be deleted automatically. This command will not be able to set the AP to create the sub-interface of the WAN port in dial-up mode.

【Configuration Example】 1: Use the show ap-config running command to check whether the configuration is successful.

```
AC-FS(config)# ap-config AP1
AC-FS(config-ap)# no ap-subif enable
```

【Prompt Information】-

【Common Mistake】-

【Platform Description】 Only AC supports this command

10.2 ap-vlan

Configure the native VLAN of the AP, and the AP will transmit the frames under this VLAN in the form of UNTAG.

ap-vlan vlan-id

Restore Defaults.

no ap-vlan

【Parameter Description】

Parameter	Description
vlan-id	Configure the VLAN used by the wired network interface. vlan-id: The specified VLAN, the value range is 1~4094, the default value is 1.

【Default Configuration】 The default value is 1.

【Command Mode】 AP configuration mode/all AP configuration mode

【Default Level】 15

【Usage Guide】 The AP will automatically strip the TAG of the frame with the Native VLAN and then forward it, that is, in the local forwarding mode, when the user's VLAN is the same as the Native VLAN, the user's frame will be forwarded without the TAG, and the access switch will forward the frame. Determines the VLAN to which the user belongs.

1. Configuring this command will disconnect and rebuild the AP that is already online.

2. In WDS deployment, when both ROOT-BRIDGE and NONROOT-BRIDGE devices deploy local forwarding, the same AP-VLAN needs to be planned, otherwise the NONROOT-BRIDGE device will not be able to share the same address pool with Normal forwarding of BRIDGE device packets.

3. This command only needs to be configured in the local forwarding mode, if the STA and AP are in the same subnet, and the VLAN of the STA and AP has been deployed. This configuration is generally not required.

4. If a static DHCP address pool is configured and the client ID is specified to use the BVI 1 interface, configuring this command will cause the AP's.

The BVI interface has changed, so the configuration of the DHCP server needs to be revised, otherwise the address will not be obtained.

5. When the AP uses PPPoE dial-up to obtain the address, then CAPWAP will select dialer 1 as the source interface, the STA traffic will not be forwarded with TAG, and this command is meaningless.

【Configuration Example】 The following example sets the Native VLAN for AP 1 to 20.

```
AC-FS(config)# ap-config AP1
AC-FS(config-ap)# ap-vlan 20
```

【Verification】1: Use the show ap-config running command to check whether the configuration is successful.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 AC supports this command

10.3 pass-vlan

When intelligent score + AP cascade or ring network, configure the transmission vlan of the AP host, so that when the users of different AP hosts plan a different vlan, the user message can be forwarded through the upper AP host

pass-vlan vlan-range

Restore the default value.

no pass-vlan vlan-range

【Parameter Description】

Parameter	Description
vlan-range	A list of VLAN ID ranges, you can specify multiple VLAN IDs, separated by commas or dashes. A comma separates two VLAN IDs, and a horizontal bar represents two VLAN ID ranges.

【Command Mode】 AP configuration mode

【Default Configuration】 Default not configured.

【Default Level】 15

【Usage Guide】1. This command is configurable for all AP, but the configuration only works on Smart Points + AP hosts.

2. This configuration will create the corresponding vlan on the host of Smart Points + AP, allowing the host to forward the message of the corresponding vlan. At the same time, the pass-vlan is automatically trimmed at the lower port of the host to prevent the broadcast group of other hosts from flooding to the lower micro AP of the host.

The vlan specified in this configuration cannot conflict with the vlan specified by the interface-mapping, ap-vlan, and wired-vlan commands, nor can the vlan 2444 for the internal management of Zhifen+AP be configured.

【Configuration Example】 Configure the transport VLAN for AP1 to use the VLAN 20.

```
AC-FS(config)# ap-config AP1
AC-FS(config-ap)# pass-vlan 20
```

【Verification】 Use the **show ap-config running** command to see if the configuration is successful.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 The AC supports this command.

10.4 wired-interface

For our AP with a wired network interface (e. g., a wall RG-AP110-W model AP provides an Ethernet port for wired network user access on the front of the product), the above wired network interface can be configured to close through the wired-interface command.By default, the wired network interface is open

wired-interface [slot slot-id [secondary]] [port port-id] enable

Turn off the wired network interface:

no wired-interface [slot slot-id [secondary]] [port port-id] enable

Restore the wired network interface on and off the default configuration:

default wired-interface [slot slot-id [secondary]] [port port-id] enable

【Parameter Description】

Parameter	Description
slot	Slot position for the micro-AP access.
slot-id	Slot position number, range 1~24.
secondary	Cascade devices under the current slot position.
port	Set up a wired network interface.
port-id	Specify a wired network interface with a value range of 1 to 4.

enable	Open the wired network interface.

【Default Configuration】 Default Configuration， The wired network interface is turned on

【Command Mode】 AP configuration mode / All AP configuration mode / AP group configuration mode

【Default Level】 15

【Usage Guide】 1. This command is configurable for all AP, but the configuration is valid only for AP models with a wired network interface.

2. When the command is configured without the port parameter, all wired network interface configurations are set up the same. When all four port configurations are turned off, the configuration displays without the port parameter. The slot parameter is only valid only for intelligence + AP, and not the slot parameter is applied to all micro AP .The secondary indicates that it takes effect for the second stage device in the cascading scenario, and without the secondary parameters for the first stage device for the non-cascading scene or the cascading scene.

3. The thin AP is started with zero configuration, and its configuration is delivered from the AC. The configuration information of the wired port is automatically saved on the AP. In this way, when the AP is disconnected from the AC, the configuration of the wired port will be restored after the AP restarts. If the wired port is configured to be closed, the wired port will still be closed after the AP restarts. When the wired port of the AP is closed, the AP cannot be managed through the wired port after restarting. At this time, you can long press the reset button of the AP to restore the factory configuration.

【Configuration Example】 Configure the AP1 to turn off the wired network interface.

```
AC-FS(config)# ap-config AP1
AC-FS(config-ap)# no wired-interface
```

【Verification】 Use the show ap-config running command to see if the configuration is successful.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 The AC supports this command.

10.5 wired-rate

Commands to configure the bandwidth limits for each LAN port:

Thin AP configuration: wired-rate value [port port-id] [slot slot-id [secondary]]

Fat AP configuration: Fat AP configuration: wired-rate value

【Parameter Description】

Parameter	Description
value	Specifies the speed limit value in 1Mbps.The default default is no speed limit. The AP each takes effect at the maximum capacity value.
port-id	Specifies the interface. The port-id is configured with 1-4 with no default value and no such parameter in fat AP mode.
slot-id	Specify the micro-AP. The slot-id is configurable 1-24 with no default and parameters are valid for Smart + AP.
secondary	Cascade devices under the current slot position

【Default Configuration】 The default is no speed limit, and AP takes effect with the maximum capability value of the AP itself.

【Command Mode】 Fit AP in the AP configuration mode or AP-GROUP configuration mode, fat AP in the interface configuration mode.

【Default Level】 15

【Usage Guide】 Command support products are detailed in the Configuration Manual. When the command does not specify a port, it indicates all LAN port rates on the configuration AP. The same configuration is applied for the lot parameter only for Smart Points + AP, and when the slot parameter is not specified for all micro AP. The secondary indicates that it takes effect for the second stage device in the cascading scenario, and without the secondary parameters for the first stage device for the non-cascading scene or the cascading scene.

【Configuration Example】 1: Configure the port 2 speed limit of 50 for a single AP.

```
AC-FS(config)# ap-config [ap-name]
AC-FS(config-ap)# wired-rate 50 port 2
```

2: Configure the port 3 speed limit of 30 for all AP.

```
AC-FS(config)# ap-config all
AC-FS(config-ap)# wired-rate 30 port 3
```

3: Interface FastEthernet 0 / 4 or GigabitEthernet 0 / 4 with fat AP 40.

```
AC-FS(config-if-FastEthernet 0/4)#wired-rate 40
```

or

```
AC-FS(config-if-GigabitEthernet 0/4)#wired-rate 40
```

4: Configure the port 1 speed limit of 80 for the group AP.

```
AC-FS(config)#ap-group default
AC-FS(config-group)#wired-rate 80 port 1
```

5: configuration group AP are 90.

```
AC-FS(config)#ap-group default
AC-FS(config-group)#wired-rate 90
```

6：The slot 3 port rate for the smart AP is 90.

```
AC-FS(config)#ap-config am5528
AC-FS(config-ap)#wired-rate 90 slot 3
```

【Verification】 Using the show run command, you can view the currently configured commands, not displayed by default.

【Prompt Information】 N/A

【Common Mistake】 N/A

【Platform Description】 Command support differences are detailed in the configuration manual.

10.6 wired-vlan

For our AP with a wired network interface (e. g., a wall RG-AP110-W model AP provides an Ethernet port for wired network user access on the front of the product), the VLAN used in the above wired network interface can be configured through the wired-vlan command. By default, the wired network interface uses the same VLAN as the AP.

wired-vlan vlan-id [slot slot-id [secondary]] [port port-id] auto-save

Restore the default value.

no wired-vlan [vlan-id [slot slot-id [secondary]] [port port-id]] auto-save

【Parameter Description】

Parameter	Description
vlan-id	Configure the VLAN used by the wired network interface. *vlan-id*: Specified VLAN with a value range from 1 to 4094.
slot	Slot position for the micro-AP access
slot-id	Slot position number, range 1~24
secondary	Cascade devices under the current slot position
port	Set up a wired network interface
port-id	Specify a wired network interface with a value range of 1 to 4.
auto-save	Save the configuration on the AP, and it can be restored after the device restart

【Default Configuration】 The default is not configured, indicating that the wired network interface uses the same VLAN as the AP

【Command Mode】 AP configuration mode / All AP configuration mode / AP group configuration mode

【Default Level】 15

【Usage Guide】 1. This command is configurable for all AP, but the configuration is valid only for AP models with a wired network interface.

2. When the command is configured without the port parameter, all wired network interfaces are set to the same VLAN. When the configuration of four port's belong to the same VLAN, the configuration displays without the port parameter. The lot parameter is valid only for the wise score + AP, and the same configuration is applied to all micro AP without the specified slot parameter. The secondary indicates that it takes effect for the second stage device in the cascading scenario, and without the secondary parameters for the first stage device for the non-cascading scene or the cascading scene.

3. In wireless AP mode (AP only does wireless access, not assigns an address to the user), when the VLAN used with the wired network interface is the same as the AP, the VLAN of the cable port message will be determined by the access switch rather than the vlan specified in this configuration. When the message of the wired network interface needs to be forwarded with TAG, the Native VLAN of the access switch cannot be the same as the VLAN of the wired network interface, otherwise the message cannot be forwarded to the wired network interface.

4. In wire routing mode (AP can assign addresses to the user), the wired user will obtain the address from the DHCP address pool on the AP, and the VLAN corresponding to the interface where the address pool is is the same as the VLAN specified by the command.

5. The Thin AP is a zero-configuration hoist, and its configuration is issued from the AC. You can configure the auto-save parameter so that the configuration information for the wired port is automatically saved on the AP. This way that when AP and AC are disconnected, the AP restart will restore the wired port configuration, so that the user can still access the network through the wired port.

When the wired port configuration can be saved and the Native VLAN of the wired port VLAN is different from the AP, if the address cannot be obtained after the AP restart, it cannot be managed through the wired port. At this time, you can long press the reset key of the AP to restore the factory configuration.

【Configuration Example】 The wired network interface for configuring the AP1 uses the VLAN 20.

```
AC-FS(config)# ap-config AP1
AC-FS(config-ap)# wired-vlan 20
```

【Verification】 Use the show ap-config running command to see if the configuration is successful.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 The AC supports this command.

11 PoE

11.1 poe enable

Configure the port-based PoE external enabling capability for the specified AC .

poe enable

Configure the specific port-based PoE feature to turn off the AC.

no poe enable

【Default Configuration】 The default individual ports enable externally.

【Command Mode】 Configuration mode of the AC under each port

【Default Level】 14

【Usage Guide】 This command is used to configure the port-based PoE functionality for the AC, which is not supported for ports that do not support the PoE.

【Configuration Example】 1: Configure the port GigabitEthernet 0 / 1-based PoE functionality for the specified AC.

```
AC-FS(config-if-GigabitEthernet 0/1)#poe enable
```

2: Turn off the P-based PoE functionality of AP.

```
AC-FS(config-if-GigabitEthernet 0/1)#no poe enable
```

【Verification】 Use the show running config command on the AC to view the configuration parameters for the global (AC) -based PoE.

【Prompt Information】 The command can be configured under a port not supported, the command cannot be entered.

【Common Mistake】 -

【Platform Description】 This command is supported only on the wireless AC product AC-64.

Chapter 2 WLAN RF

This volume introduces the relevant contents of WLAN RF command manual, including the following chapters:

1. RRM
2. RRM2. 0
3. RF dispatching
4. Spectrum navigation
5. 5. 802.11KV

1 RRM

1.1 advanced 802.11 factory

Restore all RRM configurations as a default value

advanced { 802.11a | 802.11b } factory

【Parameter Description】

Parameter	Description
802.11a	The 5G frequency band network.
802.11b	The 2.4G frequency band network.

【Default Configuration】 -

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example】 Restore all RRM configurations for the 2.4G frequency band network to the default value

```
AC-FS(config)#advanced 802.11b factory
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.2 advanced 802.11 logging channel

Log switch for channel adjustment.

advanced { 802.11a | 802.11b } logging channel { on | off }

Delete the current configuration.

no advanced { 802.11a | 802.11b } logging channel

Restore Default Configuration.

default advanced { 802.11a | 802.11b } logging channel

【Parameter Description】

Parameter	Description
802.11a	The 5G frequency band network.
802.11b	The 2.4G frequency band network.
on	Open the log for channel adjustment.
off	Close the log for channel adjustment.
default	Restore the default configuration.

【Default Configuration】 Default is closed.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example】 Open the channel auto log for the 2.4G band network.

```
AC-FS(config)#advanced 802.11b logging channel on
```

【Verification】 Use the **show advanced {802.11a | 802.11b}** logging command to view the RRM log switch.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.3 advanced 802.11 logging coverage

Log switch for customer crossing reports.

advanced { 802.11a | 802.11b } logging coverage { on | off }

elete the current configuration.

no advanced { 802.11a | 802.11b } logging coverage

Restore the Default Configuration.

default advanced { 802.11a | 802.11b } logging coverage

【Parameter Description】

Parameter	Description
802.11a	The 5G frequency band network.
802.11b	2.4G, the frequency band network.
on	Open the log for customer number violation reports
off	Close the log for customer violation reports.
default	Restore the Default Configuration.

【Default Configuration】 Default is closed.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example】 Open the log for the customer crossing report for the 2.4G band network.

```
AC-FS(config)#advanced 802.11b logging coverage on
```

【Verification】 Use the show advanced {802.11a | 802.11b} logging command to view the RRM log switch.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.4 advanced 802.11 logging foreign

AP interference log switch for the crossing report.

advanced { 802.11a | 802.11b } logging foreign { on | off }

Delete the current configuration.

no advanced { 802.11a | 802.11b } logging foreign

Restore the Default Configuration.

default advanced { 802.11a | 802.11b } logging foreign

【Parameter Description】

Parameter	Description
802.11a	The 5G frequency band network.
802.11b	The 2.4G frequency band network.
on	Open the log for the load crossing report.
off	Close the log for the load-crossing report.
default	Restore the default configuration.

【Default Configuration】 Default is closed

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example】 Open the log for the AP interference report for the 2.4G band network.

```
AC-FS(config)#advanced 802.11b logging foreign on
```

【Verification】 Use the show advanced {802.11a | 802.11b} logging command to view the RRM log switch.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.5 advanced 802.11 logging load

Log switch for the load transgression report

advanced { 802.11a | 802.11b } logging load { on | off }

Delete the current configuration.

no advanced { 802.11a | 802.11b } logging load

Restore the Default Configuration.

default advanced { 802.11a | 802.11b } logging load

【Parameter Description】

Parameter	Description
802.11a	The 5G frequency band network.
802.11b	The 2.4G frequency band network.
on	Open the log for the load crossing report.
off	Close the log for the load-crossing report.
default	Restore the default configuration.

【Default Configuration】 Default is closed.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example】 Open the log for the load crossing report for the 2.4G band network.

```
AC-FS(config)#advanced 802.11b logging load on
```

【Verification】 Use the show advanced {802.11a | 802.11b} logging command to view the RRM log switch.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.6 advanced 802.11 logging noise

Log switch for channel noise crossing report.

advanced { 802.11a | 802.11b } logging noise { on | off }

Delete the current configuration.

no advanced { 802.11a | 802.11b } logging noise

Restore the Default Configuration.

default advanced { 802.11a | 802.11b } logging noise

【Parameter Description】

Parameter	Description
802.11a	The 5G frequency band network.
802.11b	The 2.4G frequency band network.
on	Open the log for channel noise crossing report.
off	Close the log for the channel noise crossing report.
default	Restore the default configuration.

【Default Configuration】 Default is closed.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example】 Open the log for the channel noise overline report for the 2.4G frequency band network.

```
AC-FS(config)#advanced 802.11b logging noise on
```

【Verification】 Use the show advanced {802.11a | 802.11b} logging command to view the RRM log switch.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.7 advanced 802.11 logging performance

Log switch for performance violation reports.

advanced { 802.11a | 802.11b } logging performance { on | off }

Delete the current configuration.

no advanced { 802.11a | 802.11b } logging performance

Restore the Default Configuration.

default advanced { 802.11a | 802.11b } logging performance

【Parameter Description】

Parameter	Description
802.11a	The 5G frequency band network.
802.11b	The 2.4G frequency band network.
on	Open the log for channel noise crossing report.
off	Close the log for the channel noise crossing report.
default	Restore the default configuration.

【Default Configuration】 Default is closed

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example】 Open the log for the performance violation report for the 2.4G frequency band network.

```
AC-FS(config)#advanced 802.11b logging performance on
```

【Verification】 Use the show advanced {802.11a | 802.11b} logging command to view the RRM log switch.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.8 advanced 802.11 logging txpower

Log switch for automatic power control.

advanced { 802.11a | 802.11b } logging txpower { on | off }

Delete the current configuration.

no advanced { 802.11a | 802.11b } logging txpower

Restore the Default Configuration.

default advanced { 802.11a | 802.11b } logging txpower

【Parameter Description】

Parameter	Description
802.11a	The 5G frequency band network.
802.11b	The 2.4G frequency band network.
on	Open the log for channel noise crossing report.
off	Close the log for the channel noise crossing report.
default	Restore the default configuration.

【Default Configuration】 Default is closed

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example】 Open the log for the automatic power control of the 2.4G frequency band network.

```
AC-FS(config)#advanced 802.11b logging txpower on
```

【Verification】 Use the show advanced {802.11a | 802.11b} logging command to view the RRM log switch.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.9 advanced 802.11 profile clients

Configure alarm water lines for AP associated customers in global mode

advanced { 802.11a | 802.11b } profile clients { global | *ap-name* } *clients-num*

Configure the alarm waterline for AP associated customers in AP mode.

advanced { 802.11a | 802.11b } profile clients *clients-num*

Delete the current configuration in global mode.

no advanced { 802.11a | 802.11b } profile clients { global | *ap-name* }

Delete the current configuration in AP mode.

no advanced { 802.11a | 802.11b } profile clients

Recovery of the Default Configuration in global mode.

default advanced { 802.11a | 802.11b } profile clients { global | *ap-name* }

Recovery of the Default Configuration in AP mode.

default advanced { 802.11a | 802.11b } profile clients

【Parameter Description】

Parameter	Description
802.11a	The 5G frequency band network.
802.11b	2.4G, the frequency band network.

global	Specify alarm water lines for all AP in global mode.
ap-name	Specifying alarm water lines for a single AP in global mode, this parameter is not required in AP mode.
clients-num	Number of customers alarm water line, with a value range of <1-128>.
default	Restore the default configuration.

【Default Configuration】 The default value is 32.

【Command Mode】 Global mode, AP mode

【Default Level】 14

【Usage Guide】 The log is printed when the actual number of customers associated with the AP exceeds the alarm waterline, and the corresponding log switch is turned on.

【Configuration Example】 1: The number of customers in the 2.4G band network configured with all AP in global mode alarms the waterline of 20.

```
AC-FS(config)#advanced 802.11b profile clients global 20
```

2: The number of customers in the 2.4G band network named AP in AP mode alarm the water line is 25.

```
AC-FS(config)#ap-config ap2
AC-FS(config-ap)#advanced 802.11b profile clients 25
```

【Verification】 Use the show advanced {802.11a | 802.11b} profile command to view the customer alarm water lines

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.10 advanced 802.11 profile foreign

An alarm water line for AP interference in global mode.

advanced { 802.11a | 802.11b } profile foreign { global | *ap-name* } *percent*

The alarm water line with AP interference in AP mode.

advanced { 802.11a | 802.11b } profile foreign *percent*

Delete the current configuration in global mode.

no advanced { 802.11a | 802.11b } profile foreign { global | *ap-name* }

Delete the current configuration in AP mode.

no advanced { 802.11a | 802.11b } profile foreign

Recovery of the Default Configuration in global mode.

default advanced { 802.11a | 802.11b } profile foreign { global | *ap-name* }

Recovery of the Default Configuration in AP mode.

default advanced **{** 802.11a **|** 802.11b **}** profile foreign

【Parameter Description】

Parameter	Parameter
802.11a	The 5G frequency band network.
802.11b	2.4G, the frequency band network.
global	Specify alarm water lines for all AP in global mode.
ap-name	Specifying alarm water lines for a single AP in global mode, this parameter is not required in AP mode.
percent	AP interference alarm waterline in percentage, value range <1-100>.
default	Restore the Default Configuration.

【Default Configuration】 The default value is 60%.

【Command Mode】 Global mode, AP mode

【Default Level】 14

【Usage Guide】 The log is printed when the AP interference exceeds the alarm water line and the corresponding log switch is on.

【Configuration Example】 1: The AP interference alarm waterline for the 2.4G band network configured with all AP is 30.

```
AC-FS(config)#advanced 802.11b profile foreign global 30
```

2: The AP interference alarm waterline for the A 2.4G band network with A p 2 AP in AP mode is 50.

```
AC-FS(config)#ap-config ap2
AC-FS(config-ap)#advanced 802.11b profile foreign 50
```

【Verification】 Using the show advanced {802.11a | 802.11b} profile command, you can view the AP interference alarm waterline.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.11 advanced 802.11 profile noise

The alarm water line for channel noise in global mode.

advanced { 802.11a | 802.11b } profile noise { global | *ap-name* } *value*

An alarm water line for channel noise in AP mode.

advanced { 802.11a | 802.11b } profile noise *value*

Delete the current configuration in global mode

no advanced { 802.11a | 802.11b } profile noise { global | *ap-name* }

Delete the current configuration in AP mode.

no advanced { 802.11a | 802.11b } profile noise

Recovery of the Default Configuration in global mode.

default advanced { 802.11a | 802.11b } profile noise { global | *ap-name* }

Recovery of the Default Configuration in AP mode.

default advanced { 802.11a | 802.11b } profile noise

【Parameter Description】

Parameter	Parameter
802.11a	The 5G frequency band network.
802.11b	2.4G, the frequency band network.

global	Specify alarm water lines for all AP in global mode.
ap-name	Specifying alarm water lines for a single AP in global mode, this parameter is not required in AP mode.
value	Channel noise alarm waterline in dBm, range from-127 to 0.
default	Restore the default configuration.

【Default Configuration】 The default value is-70dBm.

【Command Mode】 Global mode, AP mode

【Default Level】 14

【Usage Guide】 The log is printed when the AP channel noise exceeds the alarm waterline and the corresponding log switch is on

【Configuration Example】 1：The channel noise alarm waterline for the 2.4G frequency band network of all AP configured in global mode is-80dBm.

```
AC-FS(config)#advanced 802.11b profile noise global -80
```

2：The channel noise alarm water line for the 2.4G frequency band network configured with an AP in the AP mode named ap2 is-65dBm.

```
AC-FS(config)#ap-config ap2
AC-FS(config-ap)#advanced 802.11b profile noise -65
```

【Verification】 Use the show advanced {802.11a | 802.11b} profile command to view the channel noise alarm waterline

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.12 advanced 802.11 profile throughput

An alarm water line for AP data throughput in global mode.

advanced { 802.11a | 802.11b } profile throughput { global | *ap-name* } *value*

Configure the alarm water line for the AP data throughput in AP mode.

advanced { 802.11a | 802.11b } profile throughput value

Delete the current configuration in global mode.

no advanced { 802.11a | 802.11b } profile throughput { global | ap-name }

Delete the current configuration in AP mode.

no advanced { 802.11a | 802.11b } profile throughput

Recovery of the Default Configuration in global mode.

default advanced { 802.11a | 802.11b } profile throughput { global | ap-name }

Recovery of the Default Configuration in AP mode.

default advanced { 802.11a | 802.11b } profile throughput

【Parameter Description】

Parameter	Description
802.11a	The 5G frequency band network.
802.11b	2.4G, the frequency band network.
global	Specify alarm water lines for all AP in global mode.
ap-name	Specifying alarm water lines for a single AP in global mode, this parameter is not required in AP mode.
value	AP data throughput alarm waterline in bps, value range of <1000-10000000000>
default	Restore the default configuration.

【Default Configuration】 The default value is 1500000000 bps.

【Command Mode】 Global mode, AP mode

【Default Level】 14

【Usage Guide】 The log is printed when the AP data throughput exceeds the alarm water line and the corresponding log switch is on.

【Configuration Example】 1: The data throughput alarm waterline for the 2.4G band network configured all AP in global mode is 1000000bps.

```
AC-FS(config)#advanced 802.11b profile throughput global 1000000
```

2: The data throughput alarm waterline for the 2.4G band network configured AP in AP mode named ap2 is 2000000bps.

```
AC-FS(config)#ap-config ap2
AC-FS(config-ap)#advanced 802.11b profile throughput 2000000
```

【Verification】 Use the show advanced {802.11a | 802.11b} profile command to view the AP data throughput alarm waterline.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.13 advanced 802.11 profile utilization

Configure the alarm water line for AP utilization in global mode.

advanced { 802.11a | 802.11b } profile utilization { global | *ap-name* } *percent*

Configure the alarm water line for AP utilization in AP mode.

advanced { 802.11a | 802.11b } profile utilization *percent*

Delete the current configuration in global mode.

no advanced { 802.11a | 802.11b } profile utilization { global | *ap-name* }

Delete the current configuration in AP mode.

no advanced { 802.11a | 802.11b } profile utilization

Recovery of the Default Configuration in global mode.

default advanced { 802.11a | 802.11b } profile utilization { global | *ap-name* }

Recovery of the Default Configuration in AP mode

default advanced **{** 802.11a **|** 802.11b **}** profile utilization

【Parameter Description】

Parameter	Description
802.11a	The 5G frequency band network.
802.11b	2.4G, the frequency band network.
global	Specify alarm water lines for all AP in global mode.

ap-name	Specifying alarm water lines for a single AP in global mode, this parameter is not required in AP mode.
percent	AP utilization alarm waterline in percentage, value range <1-100>.
default	Restore the default configuration.

【Default Configuration】 The default value is 80%

【Command Mode】 Global mode, AP mode

【Default Level】 14

【Usage Guide】 The log is printed when the AP utilization exceeds the alarm water line and the corresponding log switch is on.

【Configuration Example】 1: The utilization alarm water line for the 2.4G band network with all AP configured in global mode is 50%

```
AC-FS(config)#advanced 802.11b profile utilization global 50
```

2: The utilization alarm water line for the 2.4G frequency band network in AP mode configured with an AP named ap2 is 30%

```
AC-FS(config)#ap-config ap2
AC-FS(config-ap)#advanced 802.11b profile utilization 30
```

【Verification】 Use the show advanced {802.11a | 802.11b} profile command to view the AP utilization alarm waterline

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.14 advanced 802.11 txpower co-channel

Configuring whether the TPC algorithm considers only the neighbor AP of the same channel.

advanced { 802.11a | 802.11b } txpower co-channel { enable | disable }

Delete the current configuration.

no advanced { 802.11a | 802.11b } txpower co-channel

Restore the Default Configuration.

default advanced { 802.11a | 802.11b } txpower co-channel

【Parameter Description】

Parameter	Description
802.11a	The 5G frequency band network.
802.11b	2.4G, the frequency band network.
enable	Only the neighbor AP of the same channel is considered in the TPC algorithm
disable	All neighbor AP are considered in the TPC algorithm.
default	Restore the default configuration.

【Default Configuration】 The default value is disable

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example】 TPC algorithm for 2.4G band network so that only neighbor AP of the same channel is considered.

```
AC-FS(config)#advanced 802.11b txpower co-channel enable
```

【Verification】 Use the show advanced {802.11a | 802.11b} txpower command to view the automatic power control information.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.15 advanced 802.11 txpower dtpc

Power automatic control on or off (TPC).

advanced { 802.11a | 802.11b } txpower dtpc { enable | disable }

Delete the current configuration.

no advanced { 802.11a | 802.11b } txpower dtpc

Restore the Default Configuration.

default advanced { 802.11a | 802.11b } txpower dtpc

【Parameter Description】

Parameter	Description
802.11a	The 5G frequency band network.
802.11b	2.4G, the frequency band network.
enable	Turn on the automatic power control.
disable	Turn off the automatic power control.
default	Restore the default configuration.

【Default Configuration】 The default value is disable.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example】 Open the TPC algorithm for the 2.4G frequency band network.

```
AC-FS(config)#advanced 802.11b txpower dtpc enable
```

【Verification】 Use the show advanced {802.11a | 802.11b} txpower command to view the automatic power control information.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.16 advanced 802.11 txpower global

Configure the running mode of the TPC algorithm.

advanced { 802.11a | 802.11b } txpower global { auto | once | *power-level* }

Delete the current configuration.

no advanced { 802.11a | 802.11b } txpower global

Restore the Default Configuration.

default advanced { 802.11a | 802.11b } txpower globa

【Parameter Description】

Parameter	Description
802.11a	The 5G frequency band network.
802.11b	2.4G, the frequency band network.
auto	Configure the TPC algorithm as a periodic running mode.
once	Configure the TPC algorithm to trigger the running mode.
power-level	Specify the power level for all AP, with a valid value of <1-8>.
default	Restore the default configuration.

【Default Configuration】 Cycle operation mode

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 The operation mode of the TPC algorithm is divided into three types: periodic operation, trigger operation, and specified power level. When the TPC algorithm is set to cycle or trigger, the TPC algorithm is allowed only when the advanced 802.11 txpower dtpc command is set to enable. When the TPC algorithm is set to trigger the running mode, the complete TPC algorithm can be manually launched once, using advanced 802.11 txpower update .In addition, the transmit power can also be specified for all of the AP's by using the input power levels.

Level 1 corresponds to maximum emission power, level 8 corresponds to minimum emission power, and adjacent levels are halved.

【Configuration Example】 1: The TPC algorithm configthe 2.4G band network is to trigger the operation mode and manually start the algorithm once.

```
AC-FS(config)#advanced 802.11b txpower global once
AC-FS(config)#advanced 802.11b txpower update
```

2: Manually specify the transmission power level for all AP as level 1.

```
AC-FS(config)#advanced 802.11b txpower global 1
```

【Verification】 Use the show advanced {802.11a | 802.11b} txpower command to view the automatic power control information.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.17 advanced 802.11 txpower threshold

Configure the neighbor RSSI limits used by the TPC algorithm.

advanced { 802.11a | 802.11b } txpower threshold *value*

Delete the current configuration.

no advanced **{** 802.11a **|** 802.11b **}** txpower threshold

Restore the Default Configuration.

default advanced **{** 802.11a **|** 802.11b **}** txpower threshold

【Parameter Description】

Parameter	Description
802.11a	The 5G frequency band network.
802.11b	2.4G, the frequency band network.
value	Neighbor RSSI limits in dBm and range from-90 to-50.
default	Restore the default configuration.

【Default Configuration】 The default value is-60dBm.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】The smaller the neighbor RSSI limits, the easier it is to trigger the TPC to power control the interfering AP.

【Configuration Example】 The TPC algorithm configured a 2.4G band network uses a neighbor RSSI limit of-65dBm.

```
AC-FS(config)#advanced 802.11b txpower threshold -65
```

【Verification】 Use the show advanced {802.11a | 802.11b} txpower command to view the automatic power control information.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.18 advanced 802.11 txpower update

One-time TPC algorithm was manually initiated for power control.

advanced { 802.11a | 802.11b } txpower update

【Parameter Description】

Parameter	Description
802.11a	The 5G frequency band network.
802.11b	2.4G, the frequency band network.

【Default Configuration】 -

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 When the user has configured the running mode of the TPC algorithm as the trigger mode, the TPC algorithm e started once, and the running time of the algorithm is the next running cycle.

【Configuration Example】 The TPC algorithm configuring the 2.4G band network is trigger mode and the TPC algorithm is started once.

```
AC-FS(config)#advanced 802.11b txpower global once
AC-FS(config)#advanced 802.11b txpower update
```

【Verification】 Use the show advanced {802.11a | 802.11b} txpower command to view the automatic power control information.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.19 network rf-network-name

Configure the RF component group name.

network rf-network-name group-nameelete the current configuration

no network rf-network-name.

Restore the Default Configuration.

default network rf-network-name

【Parameter Description】

Parameter	Description
group-name	Radio frequency group name.
default	Restore the default configuration.

【Default Level】 14

【Usage Guide】 RF grouping is allowed only if between the AC configured with the same RF component group name.

【Configuration Example】 Configure the RF component group name to new-group.

```
AC-FS(config)#network rf-network-name new-group
```

【Verification】 Use the show advanced {802.11a | 802.11b} group command to let you view the RF component group names.

【Common Mistake】 -

【Platform Description】 -

1.20 show advanced 802.11 channel

Displays the relevant information about the DCA algorithm.

show advanced { 802.11a | 802.11b } channel

【Parameter Description】

Parameter	Description
802.11a	The 5G frequency band network.
802.11b	The 2.4G frequency band network.

【Command Mode】 Privileged mode, global mode

【Default Level】 15

【Usage Guide】 -

【Configuration Example】 View the information on the DCA algorithm for the 2.4G frequency band network.

```
AC-FS#show advanced 802.11b channel Automatic
Channel Assignment
  Radio Type..... 802.11b
  Channel Assignment Mode..... AUTO
  Channel Update Interval..... 120 seconds
  Periodic Motion (Day of A Week)..... All days
  Anchor Time (Hour of The Day)..... 20
  The Duration of DCA (By Hour)..... 24
```

```
Consider Foreign Factor.....yes
Consider Load Factor.....no
Consider Noise Factor.....no
Switch Channel When Countered.....disable
Packet Loss Rate Threshold.....100%
Clients Threshold.....0 client
Channel Assignment Leader..... 192.168.1.2
Last Run..... 11 seconds ago
DCA Sensitivity Level..... MEDIUM (15 dB)
DCA 802.11n Channel Width.....20 MHz
Auto-RF Allowed Channel List..... 1,6,11
Auto-RF Unused Channel List..... 2,3,4,5,7,8,9,10,12,13
```

Field Description：

Field	Interpretation
Radio Type	Frequency band type.
Channel Assignment Mode	The running mode of the DCA algorithm.
Channel Update Interval	The operating cycle of the DCA algorithm.
Periodic Motion	Runtime of the DCA algorithm in one week.
Anchor Time	Time when the DCA algorithm starts running in the day.
T e Duration of DCA	How long does the DCA algorithm run in the day.
Consider Foreign Factor	Whether the DCA algorithm considers the AP interference factors.
Consider Load Factor	Whether the DCA algorithm considers the load factors
Consider Noise Factor	Whether the DCA algorithm considers the channel noise factors.
Switch Channel When Countered	Whether the DCA algorithm supports channel switching when the AP is counter-fired.
Packet Loss Rate Threshold	Empty drop packet rate threshold used by the DCA algorithm
C ients Threshold	Number of customers threshold used by the DCA algorithm.
Channel Assignment Leader	The IP address of the RF packet leader AC performing the DCA algorithm.
Last Run	Time when the last time the DCA algorithm was run.
DCA Sensitivity Level	The DCA algorithm considers the sensitivity to the RF environment during channel allocation.
DCA 802.11n Channel Width	Channel bandwidth of the DCA algorithm when using an 11-n network.
Auto-RF Allowed Channel List	A list of optional channels for the DCA algorithm.
Auto-RF Un sed Channel List	List of non-optional channels for the DCA algorithm.

【Prompt Information】-

【Platform Description】-

1.21 show advanced 802.11 logging

Displays the information about the RRM log switch.

show advanced { 802.11a | 802.11b } logging

【Parameter Description】

Parameter	Description
802.11a	The 5G frequency band network.
802.11b	The 2.4G frequency band network.

【Command Mode】 Privileged mode, global mode

【Default Level】 15

【Usage Guide】 -

【Configuration Example】 View information on the RRM log switch for the 2.4G frequency band network.

```
AC-FS#show advanced 802.11b logging RF
Event and Performance Logging
  Radio Type..................................... 802.11b
  Channel Update Logging.....................Off
  TxPower Update Logging.....................Off
  Coverage Profile Logging.....................Off
  Foreign Profile Logging.....................Off
  Load Profile Logging.....................Off
  Noise Profile Logging.....................Off
```

【Field interpretation】

Field	Interpretation
Radio Type	Frequency band type.
Channel Update Logging	Log switch for channel adjustment.
TxPower Update Logging	Log switch for automatic power control.
Coverage Profile Logging	AP associated log switch for customer crossing reports.
Foreign Profile Logging	AP interference log switch for the crossing report.
Load Profile Logging	Log switch for the AP load overline report.

Noise Profile Logging	Log switch for the AP channel noise overline report.
Performance Profile Logging	Log switch for the AP data throughput overline report.

【Prompt Information】 -

【Platform Description】 -

1.22 show advanced 802.11 profile

Displays the relevant information about the RRM alarm water line

show advanced { 802.11a | 802.11b } profile { global | *ap-name* }

【Parameter Description】

Parameter	Description
802.11a	The 5G frequency band network.
802.11b	The 2.4G frequency band network.
global	Displays the RRM alarm water lines for all the AP.
ap-name	RRM alarm water line for individual AP.

【Command Mode】 Privileged mode, global mode

【Default Level】 15

【Usage Guide】 -

【Configuration Example】 view the RRM alarm water lines for all AP of the 2.4G frequency band network.

```
AC-FS#show advanced 802.11b profile global AP
Global Performance Profiles
  Radio Type..................................... 802.11b
  Interference Threshold.....................................60%
  Noise Threshold.....----------70 dBm
  RF Utilization Threshold..... 80%
  Throughput Threshold..... 150000000 bps
```

【Field interpretation】

Field	Interpretation

Radio Type	Frequency band type.
Interference Threshold	The AP interferes with the alarm water line
Noise Threshold	The AP channel noise alarm water line.
RF Utilization Threshold	AP utilization rate alarm water line.
Throughput Threshold	The AP data throughput alarms the water line
Clients Thresold	AP customer number alarm water line.

【Prompt Information】 -

【Platform Description】 -

1.23 show advanced 802.11 summary

Displays the information about the AP channels and the power.

show advanced { 802.11a | 802.11b } summary

【Parameter Description】

Parameter	Description
802.11a	The 5G frequency band network.
802.11b	The 2.4G frequency band network.

【Command Mode】 Privileged mode, global mode

【Default Level】 15

【Usage Guide】 -

【Configuration Example】 View information on channel and power for all AP of the 2.4G frequency band network.

```
AC-FS#show advanced 802.11b summary
AP Name             MAC Address     Slot ID Channel TxPower Level
------------------- --------------- ------- ------- ------------
ap1                 001a.a94e.de47  1       11*     1*(100%) ap2
00d0.f822.33aa      1       11*     2*(50%)
ap3                 001a.a9c5.8951  1       6*      2*(50%)
```

【Field interpretation】

Field	Interpretation
AP Name	AP name.
MAC Address	The MAC address of AP.
Slot ID	Radio frequency port number.
Channel	Channel values, the * number indicates the global property, allow the RRM to tune the channel
TxPower Level	Power level, the * number indicates the global attribute, allowing the RRM to adjust the work rate.

【Prompt Information】 -

【Platform Description】 -

1.24 show aadvanced 802.11 txpower

Displays the relevant information about the TPC algorithm.

show advanced { 802.11a | 802.11b } txpower

【Parameter Description】

Parameter	Description
802.11a	The 5G frequency band network.
802.11b	The 2.4G frequency band network.

【Command Mode】 Privileged mode, global mode

【Default Level】 15

【Usage Guide】 -

【Configuration Example】 View the information on the TPC algorithm for the 2.4G frequency band network.

```
AC-FS#show advanced 802.11b txpower Automatic
Transmit Power Assignment
 Radio Type..................................... 802.11b
 Dynamic Transmit Power Control Support..... disable
 Transmit Power Assignment Mode.....AUTO
 Transmit Power Update Interval..... 120 seconds
 Consider The Same Channel Neighbor Only.....No
 Transmit Power Threshold.....---------- 60 dBm
 Transmit Power Assignment Leader..... 192.169.33.2
```

【Field interpretation】

Field	Interpretation
Radio Type	Frequency band type.
Dynamic Transmit Power Control Support	Whether the automatic power control is turned on.
Transmit Power Assignment Mode	The running mode of the TPC algorithm.
Transmit Power Update Interval	The operating period of the TPC algorithm.
Consider The Same Channel Neighbor Only	Whether the TPC algorithm considers only the neighbor AP of the same channel.
Transmit Power Thresho d	Neighbor RSSI limits used by the TPC algorithm.
Transmit Power Assignment Leader	The IP address of the RF packet leader that performs the TPC algorithm.
Last Run	Time of the last run of the TPC algorithm.

【Prompt Information】 -

【Platform Description】 -

1.25 show ap auto-rf radio

Displays the RF environment information for the AP.

show ap auto-rf radio *radio-id ap-name*

【Parameter Description】

Parameter	Description
802.11a	The 5G frequency band network.
802.11b	The 2.4G frequency band network.

radio-id	The RF port number of the AP.
ap-name	AP name.

【Command Mode】 Privileged mode, global mode

【Default Level】 15

【Usage Guide】 -

【Configuration Example】 View the RF environment information for the RF port 1 called ap1.

```
AC-FS#show ap auto-rf radio 1 ap1
Number Of Slots.....2
AP Name..... ap1
Mac Address..... 00d0.f822.33aa
  Radio Type .....802.11b
  Radio Slot ID..... 1
  Monotior Mode..... ENABLED
  Noise Information
    Noise Profile..... PASSED
    (Information Updated 83 Seconds Ago)
```

Channel 1 .....---------- 98 dBm
Channel 2 .....---------- 98 dBm
Channel 3 .....---------- 98 dBm
Channel 4 .....---------- 98 dBm
Channel 5 .....---------- 98 dBm
Channel 6 .....---------- 98 dBm
Channel 7 .....---------- 98 dBm
Channel 8 .....---------- 98 dBm
Channel 9..... -98 dBm
Channel 10 .....---------- 98 dBm
Channel 11 .....---------- 98 dBm
Channel 12 .....---------- 98 dBm
Channel 13 .....---------- 98 dBm
Interfere Information
Interfere Profile.....PASSED
(Information Updated 83 Seconds Ago)
Channel 1.....1%
Channel 2..... 1%
Channel 3..... 1%
Channel 4..... 1%
Channel 5..... 1%
Channel 6.....1%
Channel 7.....1%
Channel 8.....1%
Channel 9..... 1%
Channel 10.....1%
Channel 11.....1%
Channel 12.....1%
Channel 13..... 1%
Load Information
Load Profile.....PASSED
(Information Updated 16 Seconds Ago)
Receive Utilization.....0%
Transmit Utilization.....0%

Channel Throughput.....164160 bps

Coverage Information

Coverage Profile.....PASSED

(Information Updated 72 Seconds Ago)

Load Clients.....11 clients

Pool SNR Clients.....2 clients

Client Signal Strengths

RSSI -100 dBm.....0 clients

RSSI -92 dBm.....0 clients

RSSI -84 dBm.....0 clients

RSSI -76 dBm.....2 clients

RSSI -68 dBm.....3 clients

RSSI -60 dBm.....3 clients

RSSI -52 dBm.....1 clients

RSSI -44 dBm.....2 clients

Client Signal To Noise Ratios

SNR 0 dB.....0 clients

SNR 5 dB.....2 clients

SNR 10 dB.....0 clients

SNR 15 dB.....0 clients

SNR 20 dB.....3 clients

SNR 25 dB.....2 clients

SNR 30 dB.....1 clients

SNR 35 dB.....1 clients

SNR 40 dB.....1 clients

SNR 45 dB.....0 clients

SNR 50 dB.....1 clients

SNR 55 dB.....0 clients

Nearby RADs

(Information Updated 83 Seconds Ago)

RAD fc8b.973f.d863 802.11b .....----------61 dBm on channel 1

RAD d614.4b13.9cde 802.11b .....---------- 48 dBm on channel 1

```
RAD c8d3.a32a.c8e4 802.11b .....---------- 53 dBm on channel 10
RAD c83a.351a.9d18 802.11b .....---------- 60 dBm on channel 6
RAD c83a.3517.1e70 802.11b .....---------- 60 dBm on channel 10
RAD bcf6.853e.bdc0 802.11b .....---------- 61 dBm on channel 4
RAD ace8.7b91.7c53 802.11b .....---------- 55 dBm on channel 6
RAD a815.4d2e.6ef8 802.11b .....---------- 60 dBm on channel 1
RAD 940c.6d61.7e82 802.11b .....---------- 54 dBm on channel 6
RAD 940c.6d61.7d24 802.11b .....---------- 61 dBm on channel 6
RAD 940c.6d61.7c8a 802.11b .....---------- 55 dBm on channel 13
RAD 221a.a9c5.89f3 802.11b .....---------- 34 dBm on channel 1
RAD 1cfa.68dd.b042 802.11b .....---------- 55 dBm on channel 1
RAD 1cfa.68c7.9056 802.11b .....---------- 59 dBm on channel 1
RAD 14e6.e4bc.1460 802.11b .....---------- 61 dBm on channel 6
RAD 1414.4b5c.5f58 802.11b .....---------- 60 dBm on channel 13
RAD 0c72.2cec.1be8 802.11b .....---------- 56 dBm on channel 1
RAD 00ff.ffff.ff0c 802.11b .....---------- 56 dBm on channel 6
RAD 00aa.aaaa.aaae 802.11b .....---------- 47 dBm on channel 1
RAD 0087.3298.c11c 802.11b .....---------- 57 dBm on channel 1
RAD 001a.a9c5.892d 802.11b .....---------- 58 dBm on channel 11
RAD 001a.a94a.82b9 802.11b .....---------- 49 dBm on channel 6
RAD 001a.a916.967a 802.11b .....---------- 60 dBm on channel 9
RAD 001a.a916.95a2 802.11b .....---------- 52 dBm on channel 9
```

【Field interpretation】

Field	Interpretation
Number Of Slots	Frequency band type.
AP Name	AP name.
Mac Address	The MAC address of AP.
Radio Type	Type of frequency band of the RF port.
Radio Slot ID	Radio frequency port number.
Monotior Mode	Whether the RF environment monitoring is turned on.
Noise Information	Start to display the AP channel noise information.
Noise Profile	Whether noise crossed, PASSED normal, FAILED crossed.
Interfere Information	Start displaying the AP interference information.
nterfere Profile	Whether AP interference is crossed, PASSED is normal and FAILED is crossed.
Load Information	Start displaying the AP utilization information.
Load Profile	Is utilization crossed, PASSED normal, FAILED crossed.
Receive Utilization	Receive utilization rate
Transmit Utilization	Send utilization rate.

Channel Utilization	overall availability.
Channel Throughput	Data throughput.
Coverage Information	Start displaying the customer's information.
Coverage Profile	Whether the number of customers will cross the line, PASSED is normal, and FAILED will cross the line.
Load Clients	The number of customers currently associated and have traffic.
Pool SNR Clients	Weak signal customers.
Client Signal Strengths	Start displaying the customer's signal intensity information.
Client Signal To Noise Ratios	Start displaying the customer's SNR information.
Nearby RADs	Start displaying the surrounding neighbor AP information.

【Prompt Information】 -

【Platform Description】 -

2 RRM 2.0

2.1 rrm Appoint

Select the appointment time for date time for channel and power adjustment for the online AP in the specified frequency band and range.

rrm [**2.4g** | **5g**] **appoint** *date time* [**ap-group** *group-name*]

【Parameter Description】

Parameter	Description
2.4g	The 5G frequency band network.
5g	The 2.4G frequency band network.
date	Appointment Date (format: yyyy-MM-dd)
time	Appointment time (format: hh: mm: ss)
group-name	Appointment appointment for RF adjustments for the specified ap-group

【Default Configuration】 No appointment time is available by default.

【Command Mode】 config mode

【Default Level】 14

【Usage Guide】 1. After the appointment time is configured, RRM 2.0 readjusts the channel and power to the specified frequency band and the specified range at the specified time.

2. If the 2.4G or 5G band is not specified, both bands are adjusted.

3. If the optional parameter ap-group is not configured, the whole network online AP is adjusted; otherwise, only the online AP under the specified ap-group is adjusted.

【Configuration Example】 1: The online AP of the whole network 2.4G band and 5G band network is RF adjusted at 2018-10-31 00:00:00.

```
AC-FS(config)#rrm appoint 2018-10-31 00:00:00
```

2: The online AP of the whole network 2.4G frequency band network makes RF adjustment at 2018-10-31 00:00:00.

```
AC-FS(config)#rrm 2.4g appoint 2018-10-31 00:00:00
```

3: The online AP for booking the 2.4G frequency band network under the default group is RF adjusted at 2018-10-31 00:00:00.

```
AC-FS(config)#rrm 2.4g appoint 2018-10-31 00:00:00 ap-group default
```

【Verification】 Use the show running-config command, you can see if there are adjustments and range of appointments.

【Common Mistake】 -

【Platform Description】 All AC devices

2.2 rrm channel bandwidth

Select the width selection policy for the specified band is current.

rrm [2.4g | 5g] channel bandwidth current

Select the width selection policy for the specified band is optimal.

rrm [2.4g | 5g] channel bandwidth optimal

【Parameter Description】

Parameter	Description
2.4g	The 5G frequency band network.
5g	The 2.4G frequency band network.
current	Keep the current bandwidth configuration unchanged.
optimal	Automatically select the best frequency width configuration.

【Default Configuration】 The default values of 2.4G and 5G frequency band networks both adopt the "optimal" frequency width selection strategy.

【Command Mode】 config mode

【Default Level】 14

【Usage Guide】 1: The optimal policy automatically selects the width configuration based on the type of different radio and effective channel range of the AP. The selection rules are as follows:

2.4G frequency band use HT20;

The 5G frequency band without channel restriction used the HT40;

Restricted use of Radio with channel 36-64 channels using HT40;

Restricted use of Radio with 169-HT20.

5G Radio of Wisdom + AP was performed using HT20.

2: If a 2.4G or 5G band is not specified, the configuration takes effect on both bands simultaneously.

【Configuration Example】 1: The 2.4G band and 5G band networks select the current policy

```
AC-FS(config)#rrm channel bandwidth current
```

2: The 2.4G frequency band network selects the optimal " policy

```
AC-FS(config)#rrm 2.4g channel bandwidth optimal
```

【Verification】 Use the show rrm [2.4g | 5g] summary command so that you can view the width selection policy.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 All AC devices

2.3 rrm channel dynamic enable

Turn on the channel dynamic adjustment function of the specified frequency band

rrm [2.4g | 5g] channel dynamic enable

Turn off the channel dynamic adjustment function for the specified frequency band.

no rrm [2.4g | 5g] channel dynamic enable

【Parameter Description】

Parameter	Description
2.4g	The 5G frequency band network.
5g	The 2.4G frequency band network.

【Default Configuration】 The default values of both 2.4G and 5G frequency band networks turn off the channel dynamic adjustment function.

【Command Mode】 config mode and ap-group mode

【Default Level】 14

【**Usage Guide**】1. When the channel dynamic adjustment function is turned on, the RRM 2.0 periodically checks the channel interference situation of the AP (for 5 minutes). If the channel interference situation exceeds the threshold value, then try to trigger the corresponding AP for the channel adjustment.

2. After the channel dynamic adjustment function is turned on, the trigger adjustment will override the original channel and width (width selection policy is "optimal") under ap-config, and the STA may be dropped due to switching the channel during the adjustment.

3. If a 2.4G or 5G band is not specified, the configuration takes effect on both bands simultaneously.

4.If configured in config mode, it takes effect for the entire network; if configured in ap-group mode, and only for the ap-group.In addition, the ap-group mode has higher priority than the config mode.

【**Configuration Example**】 1: Turn on the channel dynamic adjustment of the 2.4G frequency band and 5G frequency band network of the whole network.

```
AC-FS(config)#rrm channel dynamic enable
```

2: Turn off the channel dynamic adjustment of the whole network with 2.4G frequency band network.

```
AC-FS(config)#no rrm 2.4g channel dynamic enable
```

3：Turn on the channel dynamic adjustment of the 2.4G frequency band network under the default group.

```
AC-FS(config)#ap-group default
AC-FS(config-goup)#rrm 2.4g channel dynamic enable
```

【**Verification**】Use the show running-config command to let you see if the channel dynamic tuning and effect range is open.

【**Prompt Information**】 -

【**Common Mistake**】 -

【**Platform Description**】 all AC devices

2.4 rrm mode enable

Turn on the new AP RF auto-adjustment function for the specified frequency band.

rrm [2.4g | 5g] mode enable

Turn off the new AP automatic RF automatic adjustment function for the specified frequency band.

no rrm [2.4g | 5g] mode enable

【Parameter Description】

Parameter	Description
2.4g	The 5G frequency band network.
5g	The 2.4G frequency band network.

【Default Configuration】 The default value is 2.4G and 5G band networks, and the new AP radio frequency automatic adjustment function is disabled.

【Command Mode】 config mode and ap-group mode

【Default Level】 14

【Usage Guide】 1. The so-called automatic adjustment of new AP and automatic adjustment means that when the new AP is launched, the AP will trigger an RF adjustment, and when the old AP is launched back online, the original configuration is used.

2. If a 2.4G or 5G band is not specified, the configuration takes effect on both bands simultaneously.

3. If configured in config mode, it takes effect for the entire network; if configured in ap-group mode, and only for the ap-group. In addition, the ap-group mode has higher priority than the config mode.

【Configuration Example】 1: Turn off the RF automatic adjustment function of the whole network 2.4G and 5G frequency band network.

```
AC-FS(config)#no rrm mode enable
```

2: Turn off the RF automatic adjustment function of the whole network 2.4G frequency band network

```
AC-FS(config)#no rrm 2.4g mode enable
```

3: Turn on the RF automatic adjustment function of the 2.4G frequency band network under the default group.

```
AC-FS(config)#ap-group default
AC-FS(config-group)#no rrm 2.4g mode enable
```

【Verification】 Using the show running-config command, you can see whether the new AP RF auto-tuning function and effective range are turned on.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 All AC devices

2.5 rrm update

Manual trigger for automatic RF adjustment of the online AP in the specified frequency band and range

rrm [2.4g | 5g] update [ap-group *ap-group*] [channel | txpower]

【Parameter Description】

Parameter	Description
2.4g	The 5G frequency band network.
5g	The 2.4G frequency band network.
ap-group	Make RF adjustments to the specified ap-group.
channel	The channel is adjusted automatically.
txpower	Automatic power control

【Default Configuration】 -

【Command Mode】 config mode

【Default Level】 14

【Usage Guide】 1. If a 2.4G or 5G band is not specified, the configuration takes effect on both bands simultaneously.

2. If the optional parameter ap-group is not configured, RF planning for the whole network online AP; otherwise, only RF planning only for the online AP under the ap-group.

3. If the optional parameter channel is configured, only the channel and width of AP (when width policy selects "optimal") to keep the power configuration unchanged; if you configure the optional parameter txpower, only the power of AP is planned, channel and width configuration remains unchanged; if neither channel or txpower are configured, the channel, width (when width policy selects "optimal") and power of AP are planned.

4. After performing the rrm [2.4g | 5g] update [ap-group XXX] or r r m [2.4g | 5g] update [ap-group XXX] channel, the new AP RF automatic adjustment function of the corresponding frequency band is automatically opened after the end of the adjustment. If the optional parameter ap-group is not configured, it opens on the whole network (Effective in config mode); otherwise, only that ap-group is on (effective in ap-group mode).

【Configuration Example】 1: The online AP of the whole network of 2.4G and 5G frequency band networks was manually triggered to resume RF planning.

```
AC-FS(config)#rrm update
```

2: Manually trigger the online AP of the whole network 2.4G frequency band network to reconduct RF planning.

```
AC-FS(config)#rrm 2.4g update
```

3: The online AP that manually triggered the whole network 2.4G frequency band network only rechannel planning, and the power configuration remains unchanged.

```
AC-FS(config)#rrm 2.4g update channel
```

4: The online AP of the 2.4G band network under default was manually triggered for RF planning.

```
AC-FS(config)#rrm 2.4g update ap-group default
```

5: The online AP that manually triggered the 2.4G band network under the default group only rechannel planning, and the power configuration remained unchanged.

```
AC-FS(config)#rrm 2.4g update ap-group default channel
```

【Verification】 With the show rrm summary command, you can see Run Status as "Running" and after using the show rrm summary command, you can see Run Status updated to "Finish".

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 All AC devices

2.6 show rrm summary

Displays the basic configuration information under the RRM specified frequency band

show rrm [2.4g | 5g] **summary**

【Parameter Description】

Parameter	Description
2.4g	The 5G frequency band network.
5g	The 2.4G frequency band network.

【Command Mode】 Privileged mode, global mode

【Default Level】 15

【Usage Guide】 If the 2.4G or 5G band is not specified, the information for both bands is displayed.

【Configuration Example】 View information on channel and power for all AP of the 2.4G frequency band network.

```
AC-FS#show rrm 2.4g summary
Radio Resource Management
  Radio Type..................................... 2.4G
```

```
AC-FS#show rrm 2.4g summary
Radio Resource Management
  Radio Type..................................... 2.4G
```

【Field interpretation】

Field	Interpretation
Radio Type	Frequency band type.
RRM Enable Mode	Whether the whole network turns on the new AP RF automatic adjustment function.
Channel Width Strategy	Frequency width selection strategy
Channel Dynamic Enable Mode	Whether the whole network opens the channel dynamic adjustment
Run Status	The RF-adjusted operating status.

【Prompt Information】 -

【Platform Description】 All AC devices

2.7 show rrm support

Displays the online AP's support for RRM.

show rrm support

【Parameter Description】-

【Command Mode】 Privileged mode, global mode

【Default Level】 15

【Usage Guide】 -

【Configuration Example】 View online AP support for RRM.

```
AC-FS#show rrm support

AP Name                                  Mac Address    Support
-----------------------------------------------------------------
dow-730-tr.....................................0074.9c5b.2885 RRM 2.0
dwo-740                                  00d0.f822.3344 RRM 1.0
am5528-es                                00d0.f822.33e6 No Support
-----------------------------------------------------------------
```

【Field interpretation】

Field	Interpretation
AP Name	AP name.
Mac Address	The MAC address of AP.
Support	The RRM version that is supported by the AP.

【Prompt Information】 -

【Platform Description】 All AC devices

3 RF Schedule

3.1 schedule Session

Create, and apply a WLAN scheduling session.

schedule session *sid*

Delete, or cancel the WLAN scheduling session.

no schedule session *sid*

Apply the AP, AP groups to schedule the session.

schedule session *sid* [radio *radio-id* | slot {*slot-id* | all }]

Cancel the AP, AP group scheduling scheduling session.

no schedule session *sid* [radio *radio-id* / slot {*slot-id* / all }]

【Parameter Description】

Parameter	Description
sid	To create, apply, or delete A schedule session ID, take the value range [1,64] on the AC device
radio mem	To apply or remove the Radio ID of the scheduling session, take the range of values [1, the number of Radio s on the AP]. Default represents all of the Radio on the AP.
radio-id	To apply or remove the Radio ID of the scheduling session, take the range of values [1, the number of Radio s on the AP]. Default represents all of the Radio on the AP.
slot-id	To apply or remove the slot bit number for a scheduling session, the values range from 1 to 24.
all	All radio or all slot.

【Default Configuration】 The scheduling session does not exist.

WLAN or Radio does not apply scheduling sessions.

【Command Mode】 Global configuration mode, WLAN configuration mode, AP configuration mode, AP group configuration mode

【Default Level】 14

【Usage Guide】 With the RF scheduling feature, you must first create a schedule session in global configuration mode before the time parameter for the scheduling session can be configured; the command does not work if the scheduling session is already created.

After the scheduling session is created, you can specify the scheduling session applied on the WLAN in the WLAN configuration mode, the scheduling session applied on the AP configuration mode, the scheduling session applied on the AP group in the AP group configuration mode; and the scheduling session applied on the AP on the fat AP interface configuration mode. Scheduling session applied on AP can specify the Radio ID or Slot parameter which by default is applied to all Radio and not to on the Slot parameter.

If the scheduling session is deleted in the global configuration mode, the scheduling session applied to the WLAN, AP, and AP group is automatically deleted.

The slot Parameter is only valid for Zhifen+ products. If this parameter is specified, the micro AP will be powered off automatically.

【Configuration Example】 1: Create a scheduling session 1.

```
AC-FS(config)# schedule session 1
```

2: Apply the scheduling session 1 on the WLAN 1

```
AC-FS(config)# wlan-config 1
AC-FS(config-wlan)# schedule session 1
```

3: Apply the scheduling session 1 on the AP (AP name "ap1").

```
AC-FS(config)# ap-config ap1
AC-FS(config-ap)# schedule session 1
```

4: Apply scheduling session 1 on Radio 1 of the AP (AP name "ap1").

```
AC-FS(config)# ap-config ap1
AC-FS(config-ap)# schedule session 1 radio 1
```

5: Apply the scheduling session 1 on the AP group.

```
AC-FS(config)# ap-group default
AC-FS(config-ap-group)# schedule session 1
```

6: Apply the scheduling session 1 on the AP group Radio 1.

```
AC-FS(config)# ap-group default
AC-FS(config-ap-group)# schedule session 1 radio 1
```

7: Apply the scheduling session 1 on all the AP.

```
AC-FS(config)# ap-config all
AC-FS(config-ap)# schedule session 1
```

【Verification】 1: Using the show running-config command, you can view the configuration of the scheduling session and the scheduling session application configuration on the WLAN, AP groups.

2: Using the show ap-config running command, you can view the scheduling session application configuration on the AP

【Prompt Information】 1. First time to create a scheduling session, prompted to create a message.

```
AC-FS(config)# schedule session 1
Session 1 is created now.
```

2: If no scheduling session is applied on the WLAN, AP, or AP groups, the prompt scheduling session does not exist.

```
AC-FS(config)# wlan-config 1 AC-FS(config-
wlan)# schedule session 4
Session 4 does not exist!
```

【Common Mistake】 Apply a schedule session ID that was not created or deleted on the WLAN, AP, or AP group.

【Platform Description】 -

3.2 schedule session time-range

Configure the scheduling session time period.

schedule session *sid* time-range *n* period {everyday | *day1* [to *day2*]} time {all-day | *hh1:mm1* to *hh2:mm2*}

Delete the scheduled session time period.

no schedule session *sid* time-range *n*

【Parameter Description】

Parameter	Description

sid	Schedule session ID, value range [1,64] on AC device, value range [1,64] on fat AP device [1,8].
n	Schedule the session time period number, and take the value range [1,8].
day1	The period of the session period, day1 indicates the start date of the scheduling cycle.Date valid value { sun | mon | tue | wed | thu | fri | sat }.
to day2	day2 indicates the scheduling cycle end date. to day2 default indicates that the scheduling time period is only one day long.
everyday	In means that the scheduling period is daily, is a simplification of period sun to sat .
time hh1:mm1 to hh2:mm2	Scheduling session time range: hh1: mm1 and hh2: mm2 are the start and end times, respectively Hours and minutes of the year. Hour value range [0,23], and minute value range [0,59].
all-day	Represents that the schedule is a whole day, a simplification of time 00:00 to 23:59.

【Default Configuration】 The scheduled session time period is empty.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 After the scheduling of the session is created, you should first specify the scheduling time period.

Each scheduling session can be configured with up to eight time periods, each containing the time of scheduling and the date when that time takes effect, multiple times and periods can overlap, and overlapping time schedules also take effect.

If the end time is less than the start time, the end time is automatically assumed to be the next day's time.

If the end date of the scheduling period is before the start date, the end date is automatically assumed to be the next week's date.

【Configuration Example】 1: The scheduling time for scheduling session 1 is 21:30 per day to 8:50 the next day.

```
AC-FS(config)# schedule session 1 time-range 1 period sun to sat time 21:30 to 8:50
```

2: The scheduling times for the configuration scheduling session 1 are 22:00 on weekdays to 6:00 on the second day and 18:00 to 9:00 on the next day.

```
AC-FS(config)# schedule session 1 time-range 1 period mon to fri time 22:00 to 6:00
AC-FS(config)# schedule session 1 time-range 2 period sat to sun time 18:00 to 9:00
```

3: The scheduling times for configuring the scheduling session 1 are 10:00 to 12:00 on Monday, Wednesday, and Friday.

```
AC-FS(config)# schedule session 1 time-range 1 period mon time 10:00 to 12:00 AC-FS(config)# schedule session 1
time-range 2 period wed time 10:00 to 12:00
AC-FS(config)# schedule session 1 time-range 3 period fri time 10:00 to 12:00
```

【Verification】 1: Using the **show schedule session** command, you can view the time period configuration for the scheduling .

【Prompt Information】 If you schedule a time period of session, the new configuration overrides the original configuration. (No Prompt Information's).

【Common Mistake】 -

【Platform Description】 -

3.3 show schedule session

View the scheduling session-related configuration.

show schedule session [*sid*]

【Parameter Description】

Parameter	Description
sid	Schedule session ID to view, take the value range [1,64]. Default means viewing all created scheduling session.

【Command Mode】 Privilege mode

【Default Level】 1

【Usage Guide】 After the scheduling session is created, first specify the time period for scheduling.

Each scheduling session can be configured with up to 8 time periods. Each time period includes the scheduled time and the effective date of the time. The time and period of multiple time periods can overlap, and overlapping time scheduling also takes effect.

If the end time is less than the start time, the end time is automatically assumed to be the next day's time.

If the end date of the scheduling period is before the start date, the end date is automatically assumed to be the next week's date.

【Configuration Example】 View all of the scheduling session configurations.

```
AC-FS# show schedule session
Schedule Session 1:
  time-range 1 period mon time 10:00 to 12:00
  time-range 2 period wed time 10:00 to 12:00
Schedule Session 2:
  time-range 1 period Sun to Sat time 00:00 to 09:00
```

Field	interpretation
Schedule Session	Schedule the session ID's.
time-range	Time period configuration for scheduling the session.
period	he period of the time period for scheduling the session.
time	The time period for scheduling the session.

【Prompt Information】 -

【Platform Description】 -

【Field interpretation】 -

4 Band Select

4.1 band-select acceptable-rssi

Use this command to configure an acceptable STA RSSI lower limit. Use the no form of this command to restore the default setting.

band-select acceptable-rssi *value*

no band-select acceptable-rssi

【Parameter Description】

Parameter	Description
value	Indicates acceptable STA RSSI lower limits, in the range from -100 to -50 in the unit of dBm.

【Command Mode】 Global configuration mode

【Default Level】 14

【Default Configuration】 The default is -80 dBm.

【Usage Guide】 This lower limit value is used to differentiate associable STAs from non-associable STAs. If the RSSI value is greater than this value, such STAs are associable and their information will be paid attention to. If the RSSI value is less than this value, the information of such STAs will be ignored. It is not recommended that users modify the default value.

The coverage of the 2.4G band generally exceeds the coverage of the 5G band with the same signal strength. If the dual-band STA is far away from the AP and the signal strength is weak and does not want to access the 5G band, you can appropriately increase this threshold.

【Configuration Example】 The following example sets the acceptable STA RSSI low limit to -70 dBm.

```
AC-FS(config)# band-select acceptable-rssi -70
```

【Verification】 1: Use the show running-config command to view the acceptable signal strength configuration for spectrum navigation.

2: Use the show band-select configuration command to view the acceptable signal strength configuration for spectrum navigation.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

4.2 band-select access-denial

Use this command to set the access-denial count. Use the no form of this command to restore the default setting. band-select access-denial value.

no band-select access-denial

【Parameter Description】

Parameter	Description
value	Sets the access-denial count, in the range from 0 to 10.

【Command Mode】 Global configuration mode

【Default Level】 14

【Default Configuration】 The default is 2.

【 Usage Guide 】 The number of times that spectrum navigation rejects dual-frequency STAs to access the 2.4G frequency band determines the degree to which spectrum navigation inhibits the behavior of dual-frequency STAs accessing the 2.4G frequency band. It starts to respond after n link authentication requests.

Configuring this value can improve the success rate of spectrum navigation, but it may cause access difficulties for some dual-frequency STAs.

【Configuration Example】 The following example sets the access-denial count to 4.

```
AC-FS(config)# band-select access-denial 4
```

【Verification】1: Use the show running-config command to view the number of times that the dual-band STA is denied access to the 2.4G frequency band by spectrum navigation.

2: Using the show band-select configuration command, you can view the number of times the dual-band STA is denied access to the 2.4G frequency band by spectrum navigation.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.3 band-select age-out

Configure the aging time of STA information.

band-select age-out { dual-band value | suppression value }

Restore the aging time of STA information to the default value.

no band-select age-out { dual-band | suppression }

【Parameter Description】

Parameter	Description
dual-band value	The aging cycle of dual-band STA information, in the range from 20 to 120 in the unit of seconds.
suppression value	The aging cycle of suppressed STA information, in the range from 10 to 60 in the unit of seconds.

【Default Configuration】 dual-band: 60 seconds

suppression: 20 seconds

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 STA's information aging time, that is, the STA's information life cycle, the longer the cycle, the less sensitive the AP is to the STA's frequency band switching. If the wireless user's network card frequently switches between the 2.4G and 5G frequency bands (the user disables, enables the wireless network card's frequency band support), a smaller value can be configured; conversely, if the wireless user's network card does not frequently switch between the 2.4G and 5G frequency bands switch between, you can configure a larger value.

It is recommended that the information aging time of the dual-band STA be configured to be twice to three times the information aging time of the suppressed STA.

【Configuration Example】 The following example sets the aging cycle of dual-band STA information to 120 seconds.

```
AC-FS(config)# band-select age-out dual-band 120
```

The following example sets the aging cycle of suppressed STA information to 60 seconds.

```
AC-FS(config)# band-select age-out suppression 60
```

【 Verification 】 1: Use the show running-config command to view the aging time configuration of the spectrum navigation STA information.

2: Use the show band-select configuration command to view the aging time configuration of the spectrum navigation STA information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.4 band-select enable

Enable the spectrum navigation function.

band-select enable

Turn off spectrum navigation.

no band-select enable

【Parameter Description】 -

【Default Configuration】 Disable the spectrum navigation function.

【Command Mode】 WLAN configuration mode

【Default Level】 14

【Usage Guide】 To enable spectrum navigation, two conditions must be met:

1: The AP mapped by the WLAN is a dual-band AP.

2: The WLAN is mapped to two Radios of the dual-band AP at the same time.

If the application scenario does not meet these two conditions, it is recommended not to enable the spectrum navigation function of the WLAN.

If a WLAN with spectrum navigation enabled is mapped to a single-band 2.4G AP, dual-band STAs within the coverage of the AP will not be able to navigate to the 5G band.

【Configuration Example】 The following example enables the spectrum navigation for WLAN1.

```
AC-FS(config)# wlan-config 1
AC-FS(config-wlan)# band-select enable
```

The following example disables the spectrum navigation for WLAN1.

```
AC-FS(config)# wlan-config 1
AC-FS(config-wlan)# no band-select enable
```

【Verification】1: Use the show running-config command to check whether the spectrum navigation function of all WLANs is enabled or disabled.

2: Use the show wlan-config cb wlan-id command to check whether the spectrum navigation function of a WLAN is enabled or disabled.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.5 band-select he-radio access-denial

Configure the number of times that high-performance navigation STAs are denied access to non-matching frequency bands.

band-select he-radio access-denial value

The number of times of rejecting high-performance navigation STAs to access non-matching frequency bands is restored to the default value.

no band-select he-radio access-denial

【Parameter Description】

Parameter	Description
value	Configure the number of times to deny dual-band STA access to the 2.4G frequency band, the range is [0, 10].

【Default Configuration】 2

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】The number of times that high-efficiency RF navigation rejects non-HIGH-STA access to HE-RADIO (high-efficiency radio frequency) determines the degree to which high-efficiency RF navigation suppresses non-HIGH-STA access to high-efficiency radio frequency behavior: the value is n, Indicates that the AP starts to respond after receiving n consecutive link authentication requests from non-HIGH-STAs on non-high-efficiency radios.

Configuring this value can improve the success rate of high-performance RF navigation, but it may cause some STAs to have difficulty accessing.

【Configuration Example】Configure the number of times that high-performance navigation STAs are denied access to non-matching frequency bands to 4 times.

```
AC-FS(config)# band-select he-radio access-denial 4
```

【Verification】1: Use the show running-config command to view the number of times the configuration rejects high-performance navigation STAs to access non-matching frequency bands.

2: Using the show band-select configuration command, you can view the number of times the configuration rejects the high-performance navigation STA to access the non-matching band

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.6 band-select he-radio probe-count

Configure the suppression of high-efficiency navigation STAs to detect non-matching RF cycle counts.

band-select he-radio probe-count value

Recovery Suppression High Efficiency Navigation STA Detection Unmatched RF Cycle Count Value is the default value.

no band-select he-radio probe-count

【Parameter Description】

Parameter	Description
value	Configure the suppression of high-efficiency navigation STAs to detect non-matching RF cycle count values, in the range [0, 10].

【Default Configuration】 6

【Command Mode】 Global configuration mode

【Default Level】 14

【 Usage Guide 】 High-efficiency RF navigation suppresses non-HIGH-STA probe request times of HE-RADIO (high-efficiency radio frequency) determines the degree to which high-efficiency RF navigation suppresses non-HIGH-STA access to high-efficiency RF behavior: the value is n, Indicates that the AP starts the probe response after receiving n consecutive probe requests from the non-HIGH-STA on the non-high-efficiency radio frequency.

Configuring this value can improve the success rate of high-performance RF navigation, but it may cause some STAs to have difficulty accessing.

【Configuration Example】Configure the number of times that high-performance navigation STAs are denied access to non-matching frequency bands to 4 times.

```
AC-FS(config)# band-select he-radio probe-count 4
```

【Verification】1: Use the show running-config command to view the number of times the configuration rejects high-performance navigation STAs to access non-matching frequency bands.

2: Using the show band-select configuration command, you can view the number of times the configuration suppresses the high-performance navigation STA to detect non-matching frequency bands.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.7 band-select probe-count

Configure the number of times that high-performance navigation STAs are denied access to non-matching frequency bands.

band-select he-radio access-denial value

The number of times of rejecting high-performance navigation STAs to access non-matching frequency bands is restored to the default value.

no band-select he-radio access-denial

【Parameter Description】

Parameter	Description
value	Indicates the probe-count of the suppressed STAs, in the range is from 1 to 10.

【Default Configuration】 2

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This configuration item determines the degree of "suppression" of the suppressed STA: a value of n means that if the AP responds to the suppression STA's probe request once, it will not respond again until n probe cycles.

【Configuration Example】 The following example sets the probe count of the suppressed STAs to 1.

```
AC-FS(config)# band-select probe-count 1
```

【Verification】 1: Use the show running-config command to view the configuration of the detection cycle count value that inhibits STA.
2: Use the show band-select configuration command to view the configuration of the detection period count value that inhibits the STA.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.8 band-select scan-cycle

Configure the STA probe scan period threshold.

band-select scan-cycle value

Restore the STA probe scan period threshold to the default value.

no band-select scan-cycle

【Parameter Description】

Parameter	Description
value	Configure the STA probe scan period threshold, in the range [1, 1000], in milliseconds.

【Default Configuration】 200

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 The period that STA actively probes and scans WLAN on all supported channels is also the interval between two consecutive probe scans on the same channel, which is related to the drive of STA. If you clearly know the scanning period of the STA used, it is best to configure the same value to improve the recognition success rate; otherwise, use the default configuration.

If it is found that it is difficult for STAs with single-band 2.4G to discover the WLAN, the STA detection and scanning period threshold should be reduced.

【Configuration Example】 1: Configure the STA probe scan period threshold to 1 millisecond.

```
AC-FS(config)# band-select scan-cycle 1
```

【Verification】1: Use the show running-config command to view the STA probe scan cycle threshold configuration.

2: Use the show band-select configuration command to view the STA probe scan cycle threshold configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.9 show band-select configuration

Use this command to display the Band Select configuration.

show band-select configuration

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】 Use this command to view the configuration related to spectrum navigation, including: the lower limit of the acceptable STA signal strength, the number of times the dual-band STA is denied access to the 2.4G frequency band, the aging time of the STA information, and the detection period count value of the suppressed STA , the STA detects the scan cycle threshold.

【Configuration Example】 1: View the configuration related to spectrum navigation.

```
AC-FS# show band-select configuration
Band Select Configuration
  Acceptable Client RSSI (dBm)..... -80
  Access Denial Count.....0
  Age Out Dual Band (seconds).....60
  Age Out Suppression (seconds).....20
  Probe Cycle Count.....2
  Scan Cycle Period Threshold (milliseconds).....200
```

Field Description:

Field	Description
Acceptable Client RSSI	Acceptable lower limit of STA signal strength.
Access Denial Count	Number of times the dual-band STA was denied access to the 2.4G band.
Age Out Dual Band	Aging time for dual-frequency STA information.
Age Out Suppression	Suppress the aging time of STA information.
Probe Cycle Count	Suppress STA's probe cycle count value.
Scan Cycle Period Threshold	STA probe scan period threshold.

【Prompt Information】-

【Platform Description】-

4.10 show band-select statistics

Use this command to display the Band Select statistics.

show band-select statistics

【Parameter Description】

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】 Use this command to view the statistics of spectrum navigation operation.

【Configuration Example】 1: View the configuration related to spectrum navigation.

```
AC-FS# show band-select statistics
Band Select Statistics
  Number of dual band client.....4
  Number of dual band client added.....132
  Number of dual band client expired.....128
  Number of suppressed client.....6
  Number of suppressed client added.....234
  Number of suppressed client expired.....228
```

Field Description:

Field	Description
Number of dual band client	Number of current dual-band STAs.
Number of dual band client added	Number of all identified dual-frequency STAs.
Number of dual band client expired	Number of dual-band STAs that have aged out.
Number of suppressed client	Number of currently suppressed STAs.
Number of suppressed client added	Number of all identified suppressed STAs.
Number of suppressed client expired	The number of suppressed STAs that have aged out.

【Prompt Information】-

【Platform Description】-

5 802.11kv

5.1 802.11kv enable

This command is a command in global mode that opens the 802.11kv protocol interaction, including sending 802.11k beacon request, answering 802.11k neighbor report, and sending 802.11v BSS Transition.

802.11kv enable

The user can close the 802.11kv with the no option of the command

no 802.11kv enable

【Parameter Description】-

【Default Configuration】 The default is disable.

【Command Mode】 Global configuration mode.

【Default Level】 15

【Usage Guide】 Turn on the 802.11kv load balancing function and turn on the interaction with the 802.11kv protocol for the STA.

【Configuration Example】 Turn on the 802.11kv command.

```
AC-FS(config)#802.11kv enable
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

5.2 802.11kv load-balance mode

This command is off 802.11kv load balance.

802.11kv load-balance mode {none | channel-utilization | station-number}

The no command prefix is not supported.

Using the default command is available to set load balancing to an unconfigured state, and none mode is equivalent, but none is explicitly closed.

【Parameter Description】

Parameter	Description
none	Turn off the load equilibrium.
channel-utilization	Channel utilization equalization mode.
station-number	The mode of STA number equilibrium between Radio.

【Default Configuration】 The default is unconfigured, and the load equilibrium is turned off.

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】 N/A

【Configuration Example】 1: Turn off the 802.11kv load balancing.

```
AC-FS(config)#802.11kv load-balance mode none
```

2: Set the 802.11kv load mode for the channel utilization balance.

```
AC-FS(config)#802.11kv load-balance mode channel-utilization
```

3: Set the 802.11kv load mode to balance the number of STA between Radios.

```
AC-FS(config)#802.11kv load-balance mode station-number
```

【Verification】 show running

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

5.3 show 802.11kv all-bstms

This command is to view all 802.11v BSTM requests sent by the AC to all STA, including time, reason, status, and so on.

show 802.11kv all-bstms

【Parameter Description】 -

【Command Mode】 Privilege mode

【Default Level】 15

【Usage Guide】 Only data for 1024 STA were recorded and only the nearest 16 were recorded for each STA The fields displayed by the record include

WLAN: The WLAN to which the STA belongs

Time: The time of sending

Elapsed: Time experienced when sent to the STA response APMAC / Radio: The AP MAC where the STA was sent and the Radio Result: STA returned Agreed APMAC/Radio: The AP MAC that the STA reply will be switched to and the Radio Tigger Reason: AC send reason

【Configuration Example】 Displays all of the 802.11v bstm records.

```
AC-FS#show 802.11kv all-bstms
STATION:3871.de4c.8888
WLAN  Time                Elapsed  AP/Radio            Result      Agreed AP/Radio
Trigger Reason
87    2018-08-06 09:36:14  1s      0073.0000.0000/2    Refused     N/A
Station Number Load Balance
87    2018-08-06 09:35:56  1s      0073.0000.0000/1    Accepted    0073.0000.0000/2  CLI
Request
87    2018-08-06 09:35:48  0s      0073.0000.0000/1    N/A         N/A
Channel Load Balance
87    2018-08-06 09:35:37  0s      0073.0000.0000/1    N/A         N/A                CLI
Request
87    2018-08-06 09:35:17  2s      0073.0000.0000/2    Accepted    0073.0000.0000/2
Channel Load Balance
```

【Prompt Information】 -

【Platform Description】 AC

5.4 show 802.11kv bstm-per-station

This command is to view all 802.11v BSTM requests sent by the AC to a single STA, including time, reason, status, and so on.

show 802.11kv bstm-per-station *station-mac*

【Parameter Description】

Parameter	Description
station-mac	Mac of STA.

【Command Mode】 Privilege mode

【Default Level】 15

【Usage Guide】 Each STA records only the nearest 16 records showing fields included WLAN： The WLAN to which the STA belongs Time: The time of sending Elapsed: A PMAC / Radio: the AP MAC where the STA was sent and the Radio Result: STA Agreed APMAC/Radio： The AP MAC that the STA reply will be switched to and the Radio Tigger Reason: AC send reason.

【Configuration Example】 Show the 802.11v bstm record for STA 3871.de4c.8888

```
AC-FS#show 802.11kv bstms-per-station 3871.de4c.8888
WLAN  Time                Elapsed  AP/Radio          Result     Agreed AP/Radio Trigger Reason
87    2018-08-06 09:36:14 1s       0073.0000.0000/2  Refused    N/A             Station
Number Load Balance
87    2018-08-06 09:35:56 1s       0073.0000.0000/1  Accepted   0073.0000.0000/2 CLI Request
87    2018-08-06 09:35:48 0s       0073.0000.0000/1  N/A        N/A              Channel Load
Balance
87    2018-08-06 09:35:37 0s       0073.0000.0000/1  N/A        N/A                       CLI Request
87    2018-08-06 09:35:17 2s       0073.0000.0000/2  Accepted   0073.0000.0000/2 Channel Load
Balance
```

【Prompt Information】 -

【Platform Description】 AC

Chapter 3 Manual-WLAN Security

This WLAN security manual includes the following chapters:

1. RSNA
2. WIDS
3. CPP
4. NFP

1 RSNA

1.1 authtimeout forbidcount

Configure the number of times the association is prohibited after the four-way handshake key interaction fails.

authtimeout forbidcount count

Delete configuration.

no authtimeout forbidcount

Restore Default Configuration.

default authtimeout forbidcount

【Parameter Description】

Parameter	Description
count	Sets the forbid count after a four-way handshake fails to accomplish key exchange.

【Default Configuration】After the four-way handshake key exchange fails, the number of times the association is prohibited is 10.

【Command Mode】 WLAN security configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: After the configuration of the four-way handshake key interaction fails, the number of times the association is prohibited is 5 times.

AC-FS(config-wlansec)#authtimeout forbidcount 5.

【Verification】1: Use the show running-config command to check whether the configuration takes effect.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.2 authtimeout forbidtime

Configure the time interval for disabling the association after the four-way handshake key interaction fails, in seconds.

authtimeout forbidtime time

Delete configuration.

no authtimeout forbidtime

Restore Default Configuration.

default authtimeout forbidtime

【Parameter Description】

Parameter	Description
time	Sets the forbidtime after a four-way handshake fails to accomplish key exchange, in the unit of seconds.

【Default Configuration】 After the four-way handshake key exchange fails, the time interval for disabling association is 5 seconds.

【Command Mode】 WLAN security configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: After the four-way handshake key interaction fails, the time interval for disabling association is 6 seconds.

```
AC-FS(config-wlansec)#authtimeout forbidtime 6
```

【Verification】1: Use the show running-config command to check whether the configuration takes effect.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.3 authtimeout groupcount

Configure the number of retransmissions of multicast key negotiation packets.

authtimeout groupcount count

Delete configuration.

no authtimeout groupcount

Restore Default Configuration.

default authtimeout groupcount

【Parameter Description】

Parameter	Description
count	Sets the retransmission count for the multicast key negotiation packet.

【Default Configuration】 7 times.

【Command Mode】 WLAN security configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】 The following example set the retransmission count for the multicast key negotiation packet to 5.

```
AC-FS(config-wlansec)#authtimeout groupcount 5
```

【Verification】1: Use the show running-config command to check whether the configuration takes effect.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.4 authtimeout grouptime

Configure the timeout period for multicast key negotiation packets, in milliseconds.

authtimeout grouptime timeout

Delete configuration.

no authtimeout grouptime

Restore Default Configuration.

default authtimeout grouptime

【Parameter Description】

Parameter	Description
timeout	Timeout time for multicast key negotiation packets.

【Default Configuration】 1200ms.

【Command Mode】 WLAN security configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Set the timeout period for multicast key negotiation packets to 100ms.

```
AC-FS(config-wlansec)#authtimeout grouptime 100
```

【Verification】1: Use the show running-config command to check whether the configuration takes effect.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.5 authtimeout paircount

Configure the number of retransmissions of unicast key negotiation packets.

authtimeout paircount count

Delete configuration.

no authtimeout paircount

Restore Default Configuration.

default authtimeout paircount

【Parameter Description】

Parameter	Description
count	Number of retransmissions of unicast key negotiation packets.

【Default Configuration】 7 times.

【Command Mode】 WLAN security configuration mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example】 1: Set the number of unicast key negotiation packet retransmissions to 5 times.

```
AC-FS(config-wlansec)#authtimeout paircount 5
```

【Verification】 1: Use the show running-config command to check whether the configuration takes effect.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.6 authtimeout pairtime

Configure the timeout period for unicast key negotiation packets, in milliseconds.

authtimeout pairtime timeout

Delete configuration.

no authtimeout pairtime

Restore Default Configuration.

default authtimeout pairtime

【Parameter Description】

Parameter	Description
timeout	Timeout time for unicast key negotiation packets.

【Default Configuration】 1200ms.

【Command Mode】 WLAN security configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Set the unicast key negotiation packet timeout to 100ms.

```
AC-FS(config-wlansec)#authtimeout pairtime 100
```

【Verification】1: Use the show running-config command to check whether the configuration takes effect.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.7 dot1x-mab

The authentication mode for configure a WLAN is MAB authentication mode.

dot1x-mab

Turn off the MAB authentication mode

no dot1x-mab

【Parameter Description】

Parameter	Description
no	Clear the MAB authentication mode

【Command Mode】 WLAN security configuration mode

【Default Configuration】 Turn off the MAB authentication mode

【Usage Guide】 This command is used to enable MAB authentication mode and can be used simultaneously with PSK access authentication, but not with 802.1x access authentication.

【Configuration Example】 1: The authentication mode for configuring the WLAN 1 is the MAB authentication mode

```
AC-FS(config)#wlansec 1
AC-FS(config-wlansec)# dot1x-mab
```

2: Turn off the MAB authentication mode for the WLAN 1:

```
AC-FS(config)#wlansec 1
AC-FS(config-wlansec)# no dot1x-mab
```

【Prompt Information】 If the WLAN has enabled other encryption modes (such as WEP), the MAB authentication mode cannot be configured for an error.

```
now, wlan security is other security,please delete the security config first
```

【Common Mistake】 WLAN has already enabled other encryption authentication methods (such as WEP).

【Platform Description】 -

1.8 rsna lazy-response

Turn on the authentication message delay response function.

rsna lazy-response enable

Turn off the authentication message latency response function.

no rsna lazy-response enable

Restore the Default Configuration

default rsna lazy-response enable

Configure the authentication message delay response time.

rsna lazy-response timer timer

【Parameter Description】

Parameter	Description
timer	0-2000ms, default is 1000ms

【Default Configuration】 The default is on, and the show run does not display.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 On or off the authentication message delay response function, which is turned on by default. After opening, receive the auth message, and if the assoc req message is processing within 1000 ms (default), discard the new received message and continue processing the old message. If the assoc req message processing has timed out (like the default 1000 ms assoc req is not already processed), the old assoc req message is discarded and the new auth message is processed.

【Configuration Example】 1: Turn off the authentication message latency response function

```
AC-FS(config)# no rsna lazy-response enable
```

2: Configuration authentication message delay response timeout is 1500 ms

```
AC-FS(config)# rsna lazy-response timer 1500
```

【Verification】 Use the show running-config command to see if the configuration takes effect.

【Prompt Information】 N/A

【Common Mistake】 N/A

【Platform Description】 -

1.9 security rsn

Configure the authentication mode of the WLAN as RSN authentication mode.

security rsn enable

Disable RSN authentication mode.

security rsn disable

【Parameter Description】

Parameter	Description
enable	Enables the RSN authentication mode.
disable	Disables the RSN authentication mode.

【Default Configuration】 This function is disabled by default.

【Command Mode】 WLAN security configuration mode

【Default Level】 14

【Usage Guide】 The command is used to enable the RSN authentication mode. Only after the RSN authentication mode is enabled can encryption and authentication methods be configured in the RSN mode. Otherwise, any configuration is invalid. When you use the RSN authentication, you need to configure an encryption method and an authentication method. If only an encryption or authentication method is configured, or neither is configured, the wireless client cannot be associated with the wireless network. The RSN authentication mode is what is usually called WPA2 authentication mode. If both WPA and RSN authentication modes are configured simultaneously for a WLAN, the encryption and authentication methods in these two authentication modes are identical, and the newly configured encryption and authentication methods will override the previous ones.

【Configuration Example】 1. The following example sets the authentication mode of WLAN1 to RSN.

```
AC-FS(config)#wlansec 1
AC-FS(config-wlansec)#security rsn enable
```

【Verification】1: Use the show running-config command to check whether the configuration takes effect.

【Prompt Information】 1: If the WLAN has enabled other encryption methods (such as WEP), the RSN authentication mode cannot be configured, and an error is displayed.

wlan security is static wep, can't config other security mode

【Common Mistake】 1: WLAN has enabled other encryption authentication methods (such as WEP).

【Platform Description】-

1.10 security rsn akm

Configure the access authentication mode in RSN authentication mode to PSK authentication.
security rsn akm psk enable

Disable PSK access authentication in RSN authentication mode.
security rsn akm psk disable

Configure the access authentication mode in RSN authentication mode to PSK authentication.
security rsn akm psk enable

Disable PSK access authentication in RSN authentication mode.
security rsn akm psk disable

【Parameter Description】

Parameter	Description
psk	Set the access authentication mode to pre-shared key authentication.
802.1x	Set the access authentication mode to 802.1x authentication.
enable	Enable access authentication in RSN authentication mode.
disable	Disable access authentication in RSN authentication mode.

【Default Configuration】 No access authentication mode.

【Command Mode】 WLAN security configuration mode

【Default Level】 14

【Usage Guide】 This command is used to enable the authentication mode in RSN authentication mode, there are two access

authentication modes: PSK and 802.1x. The access authentication mode can be configured only when the RSN authentication mode is enabled.

Only one access authentication method can be enabled in a WLAN security configuration mode.

【Configuration Example】 1: Configure the access authentication mode in WLAN 1 RSN authentication mode as pre-shared key authentication.

```
AC-FS(config-wlansec)#security rsn akm psk enable
```

2: Configure the access authentication mode in WLAN 2 RSN authentication mode to 802.1x authentication.

```
AC-FS(config-wlansec)#security rsn akm 802.1x enable
```

【Verification】1: Use the show running-config command to check whether the configuration takes effect.

【Prompt Information】 1: If the RSN authentication is not enabled in the WLAN security configuration mode, an error will be displayed when the access authentication mode of the RSN mode is enabled.

```
AC-FS(config)#wlansec 1
AC-FS(config-wlansec)#security rsn akm psk enable
WLAN 1 rsn is disable.
```

2: If an access authentication method has been enabled in the WLAN security configuration mode, an error will be displayed when another access authentication method is enabled.

```
AC-FS(config-wlansec)#security rsn akm psk enable AC-
FS(config-wlansec)#security rsn akm 802.1x enable
Wlan 1 has config psk, can not config 1x.
```

【Common Mistake】 1: In the WLAN security configuration mode, configure the access authentication method without enabling RSN authentication.

2: In the WLAN security configuration mode, one access authentication method has been enabled, and another access authentication method cannot be configured.

【Platform Description】-

1.11 security rsn akm psk set-key

Use this command to configure a shared password for RSNs in the PSK authentication mode.

security rsn akm psk set-key { asciiascii-key|hex hex-key}

【Parameter Description】

Parameter	Description
ascii	Specifies the ASCII password.
ascii-key	The ASCII password, containing 8-63 characters.
hex	Specifies the hexadecimal password.
hex-key	The hexadecimal password, containing 64 characters.

【Default Configuration】 N/A

【Command Mode】 WLAN security configuration mode

【Default Level】 14

【Usage Guide】 This shared password takes effect only when PSK authentication is enabled. Password in ASCII code, the length is limited to 8--63 ASCII code characters. Password in hexadecimal form, must be 64 hexadecimal characters long.

【Configuration Example】 The following example sets the shared password for WLAN 1 RSN to 12345678.

```
AC-FS(config)#wlansec 1
AC-FS(config-wlansec)#security rsn enable AC-
FS(config-wlansec)#security rsn akm psk enable
AC-FS(config-wlansec)#security rsn akm psk set-key ascii 12345678
```

【Verification】1: Use the show running-config command to check whether the configuration takes effect.

【Prompt Information】 1: If the length of the password in ASCII code is less than 8 characters, it will prompt an error.

```
AC-FS(config-wlansec)#security rsn akm psk set-key ascii 1234567
ASCII PSK length must be not less than 8 (7).
```

2: If the length of the password in hexadecimal form is not 64 hexadecimal characters, an error will be prompted.

```
AC-FS(config-wlansec)# security rsn akm psk set-key hex
0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcde
Hex PSK length must be 64.
```

【Common Mistake】 1: If RSN authentication mode is not enabled, configure RSN PSK password.

2: The length of the password in ASCII code is less than 8 characters or more than 63 characters.

3: Password length in hexadecimal not 64 hexadecimal characters.

【Platform Description】-

1.12 security rsn ciphers

Configure the encryption method in RSN authentication mode to AES.

security rsn ciphers aes enable

Disable AES encryption in RSN authentication mode.

security rsn ciphers aes disable

Configure the encryption method in RSN authentication mode to TKIP.

security rsn ciphers tkip enable

Disable TKIP encryption in RSN authentication mode.

security rsn ciphers tkip disable

【Parameter Description】

Parameter	Description
aes	Configures the encryption method to AES.
tkip	Configures the encryption method to TKIP.
enable	Enables an encryption method in the RSN authentication mode.
disable	Disables an encryption method in the RSN authentication mode.

【Default Configuration】 N/A

【Command Mode】 WLAN security configuration mode

【Default Level】 14

【Usage Guide】 This command is used to enable encryption in RSN authentication mode. There are two encryption methods: AES and TKIP. In a WLAN security configuration mode, both AES and TKIP encryption methods can be enabled at the same time.

【Configuration Example】1: Configure the encryption method in WLAN 1 RSN authentication mode as AES.

```
AC-FS(config)#wlansec 1
AC-FS(config-wlansec)#security rsn enable AC-FS(config-
wlansec)#security rsn ciphers aes enable
```

【Verification】1: Use the show running-config command to check whether the configuration takes effect.

【Prompt Information】 1: If RSN authentication is not enabled in WLAN security configuration mode, an error will be displayed when configuring the encryption mode of RSN mode.

```
AC-FS(config)#wlansec 1
AC-FS(config-wlansec)#security rsn ciphers aes enable
WLAN 1 rsn is disable.
```

【Common Mistake】 1: In the WLAN security configuration mode, configure the RSN encryption method without enabling RSN authentication.

2: RSN authentication is enabled in the WLAN security configuration mode, but the encryption mode is not configured, so that the terminal cannot associate with the wireless network.

【Platform Description】-

1.13 security rsn dot11r

Configure the 802.11R feature on

security rsn dot11r enable

Turn off the 802.11R function.

security rsn dot11r disable

【Parameter Description】

Parameter	Description
enable	Turn on the 802.11R feature。
disable	Turn off the 802.11R function.

【Default Configuration】 The 802.11R feature is not turned on

【Command Mode】 The WLAN security configuration mode

【Default Level】 14

【Usage Guide】 The following conditions need to be met to open 802.11R, otherwise configure the command will fail:

- The RSN authentication mode is enabled;
- The WPA authentication mode is turned off, where both WPA and RSN are not allowed;
- The access authentication mode AKM is configured as either PSK or 802.1x;
- The AES encryption mode is enabled;
- The TKIP encryption mode is closed, where both AES and TKIP are not allowed

【Configuration Example】 1: Configure the WLAN 1-enabled 802.11R feature

```
AC-FS(config-wlansec)#security rsn dot11r enable
```

2: Configure turning off the 802.11R feature for the WLAN 2

```
AC-FS(config-wlansec)#security rsn dot11r disable
```

【Verification】 Use the show running-config command to see if the configuration takes effect.

【Prompt Information】1: If RSN authentication is not enabled in WLAN security configuration mode, an error is prompted when opening the access authentication mode in RSN mode.

```
AC-FS(config)#wlansec 1
AC-FS(config-wlansec)#security rsn dot11r enable
%ERROR% 802.11R requires RSN to be enabled, run command 'security rsn enable' first.
```

2: If the TKIP encryption mode is already enabled in the WLAN security configuration mode, an error is prompted when configuring the authentication mode of the 802.11R function.

```
AC-FS(config-wlansec)#security rsn ciphers tkip enable
AC-FS(config-wlansec)#security rsn dot11r enable
%ERROR% 802.11R requires ciphers aes to be enabled, run command 'security rsn ciphers aes enable'
first.
```

【Common Mistake】 1. 802.11R functionality is enabled without RSN authentication enabled in WLAN Security Configuration mode

2. The 802.11R functionality is enabled without AES encryption being enabled in WLAN Security Configuration mode.

3. Enables the 802.11R functionality when a WPA or TKIP configuration exists.

【Platform Description】 -

1.14 security rsn dot11r reassoc-timeout

Configure the 802.11R roaming reassociation timeout time in WLAN security configuration mode the maximum time interval when the client initiates a reassociation request after the authentication is completed.

Only 802.11R functionality is turned on

security rsn dot11r reassoc-timeout *timeout-seconds*

【Parameter Description】

Parameter	Description
timeout-seconds	Time out time length in seconds and must be an integer between 1 and 120.

【Default Configuration】 20 s

【Command Mode】 The WLAN security configuration mode

【Default Level】 14

【Usage Guide】 This command can configure the 802.11R roaming reassociation timeout time in seconds.

【Configuration Example】 The 802.11R reassociation timeout for configuring the WLAN 1 is 30s.

```
AC-FS(config)#wlansec 1
AC-FS(config-wlansec)#security dot11r reassoc-timeout 30
```

【Verification】 Use the show running-config command to see if the configuration takes effect.

【Common Mistake】 -

【Platform Description】 -

1.15 security pmf

Turn on managed frame encryption, and the client must support managed frame encryption.Clients that do not support managing frame encryption cannot be associated.

security pmf mandatory

Turn on managed frame encryption, and the client optionally supports managed frame encryption.Clients that do not support managed

frame encryption use non-encrypted managed frames.

Security pmf optional

Turn off the management frame encryption.

security pmf disable

【Parameter Description】-

【Default Configuration】 Turn off the management frame encryption.

【Command Mode】 The WLAN security configuration mode

【Default Level】 15

【Usage Guide】 None

【Configuration Example】 Configure WLAN 1 to enable managed frame encryption and requires client support

```
AC-FS(config)#wlansec 1
AC-FS(config-wlansec)# security pmf mandatory
```

【Verification】 Use the show running-config command to see if the configuration takes effect.

【Common Mistake】 In pure WPA3 mode, pmf to mandatory mode otherwise the terminal may not be accessible.

In WPA3 Personal hybrid mode, you need to configure pmf to optional mode. The configuration for the WPA3 Personal hybrid mode is WPA2 PSK + pmf optional + WPA3 SAE.At this time, both the WPA2 PSK terminal and the SAE terminal can be accessed.If you configure WPA2 PSK + pmf mandatory + WPA3 SAE, the SAE configuration does not take effect and only the supported WPA2 PSK terminals with PMF have access.

【Platform Description】 -

1.16 security static-wep-key authentication

Configure the WLAN link verification mode in static WEP mode.

security static-wep-key authentication { open | share-key }

【Parameter Description】

Parameter	Description
open	Configure the open system link verification mode
share-key	Configure the shared key link verification mode.

【Default Configuration】 The default is the open system link verification mode.

【Command Mode】 The WLAN security configuration mode

【Default Level】14

【Usage Guide】This command is used with security static-wep-key encryption and the link authentication mode is configured with the static WEP key. Security configuration mode other than static WEP mode.

【Configuration Example】 The link authentication mode for the configuration WLAN 1 is the shared key.

```
AC-FS(config-wlansec)#security static-wep-key authentication share-key
```

【Verification】 Use the show running-config command to see if the configuration takes effect.

【Prompt Information】 An error is prompted if link authentication is not configured if WEP is enabled.

```
Fail to setup WEP authmode, not in static WEP security mode (1).
```

【Common Mistake】 1: Configure the link authentication mode without enabling the static WEP mode

【Platform Description】 -

1.17 security static-wep-key encryption

Configure WLAN to enable static WEP mode while configure static WEP password.

security static-wep-key encryption *key-length* { ascii | hex } *key-index key*

【Parameter Description】

Parameter	Description
key-length	Password length, in bits, can be 40 or 104.
ascii	The password form is the ASCII code.

hex	The password form is 16 decimal characters
key-index	Key index number, the configuration range is: 1- -4.
key	code data.

【Default Configuration】 Static WEP mode is not enabled

【Command Mode】 The WLAN security configuration mode

【Default Level】 14

【Usage Guide】 This command is configuring a static WEP key while enabling a static wep mode. This command can be configured repeatedly, and the last configured command takes effect.

The key data length must be consistent with the key-length parameter specified in the command.

Only 1 WLAN can be configured with static WEP encryption mode on the device.

The static WEP mode needs to be deleted by deleting the security configuration mode of the WLAN.

【Configuration Example】 The static WEP key for configuring the WLAN 1 is 12345.

```
AC-FS(config)#wlansec 1
AC-FS(config-wlansec)#security static-wep-key encryption 40 ascii 1 12345
```

【Verification】 Use the show running-config command to see if the configuration takes effect.

【Prompt Information】 1: An error is prompted if the number of password characters does not consistent with the specified password length.

```
AC-FS(config-wlansec)#security static-wep-key encryption 40 ascii 1 123456
password Must be 5 ASCII characters.
```

2: If one WLAN on the device is already configured with static WEP mode, prompt an error when configuring another WLAN for static WEP mode.

```
Fail to setup static WEP key, because another wlan has configed static WEP.
```

【Common Mistake】 1: The number of password characters is not consistent with the specified password length.

2: Configure multiple WLAN's for the static WEP mode.

【Platform Description】 -

1.18 security wpa

Configure the authentication mode of the WLAN as WPA authentication mode.

security wpa enable

Turn off WPA authentication mode.

security wpa disable

【Parameter Description】

Parameter	Description
enable	Enables WPA authentication.
disable	Disables WPA authentication.

【Default Configuration】 WPA authentication is disabled by default.

【Command Mode】 WLAN security configuration mode

【Default Level】 14

【Usage Guide】 The command is used to enable the WPA authentication mode. Only after the WPA authentication mode is enabled can encryption and authentication methods be configured in the WPA mode. Otherwise, configuration is impossible. When you use the WPA authentication, you need to configure an encryption method and an authentication method. If only an encryption or authentication method is configured, or neither is configured, the wireless client cannot be associated with the wireless network.

【Configuration Example】1: Configure the authentication mode of WLAN 1 as WPA authentication mode.

```
AC-FS(config)#wlansec 1
AC-FS(config-wlansec)#security wpa enable
```

【Verification】1: Use the show running-config command to check whether the configuration takes effect.

【Prompt Information】 1: If the WLAN has enabled other encryption methods (such as WEP), the WPA authentication mode cannot be configured, and an error is displayed.

```
wlan security is static wep, can't config other security mode
```

【Common Mistake】 1: WLAN has enabled other encryption authentication methods (such as WEP).

【Platform Description】 -

1.19 security wpa akm

Configure the access authentication mode in WPA authentication mode to PSK authentication.

security wpa akm psk enable

Disable PSK access authentication in WPA authentication mode.

security wpa akm psk disable

Set the access authentication mode in WPA authentication mode to 802.1x authentication.

security wpa akm 802.1x enable

Disable 802.1x access authentication in WPA authentication mode.

security wpa akm 802.1x disable

【Parameter Description】

Parameter	Description
psk	Set the access authentication mode to pre-shared key authentication.
802.1x	Set the access authentication mode to 802.1x authentication.
enable	Enable access authentication in WPA authentication mode.
disable	Disable access authentication in WPA authentication mode.

【Default Configuration】 No access authentication mode.

【Command Mode】 WLAN security configuration mode

【Default Level】 14

【Usage Guide】 This command is used to enable the authentication mode in WPA authentication mode. There are two access authentication modes: PSK and 802.1x. The access authentication mode can be configured only when the WPA authentication mode is enabled.

Only one access authentication method can be enabled in a WLAN security configuration mode.

【Configuration Example】1: Configure the access authentication method in WLAN 1 WPA authentication mode to pre-shared key authentication.

```
AC-FS(config-wlansec)#security wpa akm psk enable
```

2: Configure the access authentication mode in WLAN 2 WPA authentication mode to 802.1x authentication.

```
AC-FS(config-wlansec)#security wpa akm 802.1x enable
```

【Verification】1: Use the show running-config command to check whether the configuration takes effect.

【Prompt Information】 1: If the WPA authentication is not enabled in the WLAN security configuration mode, an error will be displayed when the access authentication mode of the WPA mode is enabled.

```
AC-FS(config)#wlansec 1
AC-FS(config-wlansec)#security wpa akm psk enable
WLAN 1 wpa is disable.
```

2: If an access authentication method has been enabled in the WLAN security configuration mode, an error will be displayed when another access authentication method is enabled.

```
AC-FS(config-wlansec)#security wpa akm psk enable
AC-FS(config-wlansec)#security wpa akm 802.1x enable
Wlan 1 has config psk, can not config 1x.
```

【Common Mistake】 1: In the WLAN security configuration mode, configure the access authentication method without WPA authentication enabled.

2: In the WLAN security configuration mode, one access authentication method has been enabled, and another access authentication method cannot be configured.

【Platform Description】-

1.20 security wpa akm psk set-key ascci

Use this command to configure a WPA shared password for a WLAN.

security wpa akm psk set-key { asciiascii-key|hex hex-key}

【Parameter Description】

Parameter	Description
ascii	Specifies the ASCII password.
ascii-key	The ASCII password, containing 8-63 characters.
hex	Specifies the hexadecimal password.
hex-key	The hexadecimal password, containing 64 characters.

【Default Configuration】 N/A

【Command Mode】 WLAN security configuration mode

【Default Level】 14

【Usage Guide】 This shared password takes effect only when PSK authentication is enabled. Password in ASCII code, the length is limited to 8--63 ASCII code characters. Password in hexadecimal form, must be 64 hexadecimal characters long.

【Configuration Example】 The following example sets the shared password for WLAN 1 WPA to 12345678.

```
AC-FS(config)#wlansec 1
AC-FS(config-wlansec)#security wpa enable AC-
FS(config-wlansec)#security wpa akm psk enable
AC-FS(config-wlansec)#security wpa akm psk set-key ascii 12345678
```

【Verification】 1: Use the show running-config command to check whether the configuration takes effect.

【Prompt Information】 1: If the length of the password in ASCII code is less than 8 characters, it will prompt an error.

```
AC-FS(config-wlansec)#security wpa akm psk set-key ascii 1234567
ASCII PSK length must be not less than 8 (7).
```

2: If the length of the password in hexadecimal form is not 64 hexadecimal characters, an error will be prompted.

```
AC-FS(config-wlansec)# security wpa akm psk set-key hex
```

【Common Mistake】 1: If the WPA authentication mode is not enabled, configure the WPA PSK password.

2: The length of the password in ASCII code is less than 8 characters or more than 63 characters.

3: Password length in hexadecimal not 64 hexadecimal characters.

【Platform Description】 -

1.21 security wpa ciphers

Configure the encryption method in WPA authentication mode to AES.

security wpa ciphers aes enable

Disable AES encryption in WPA authentication mode.

security wpa ciphers aes disable

Configure the encryption method in WPA authentication mode to TKIP.

security wpa ciphers tkip enable

Disable TKIP encryption in WPA authentication mode.

security wpa ciphers tkip disable

【Parameter Description】

Parameter	Description
aes	Configures the encryption method to AES.
tkip	Configures the encryption method to TKIP.
enable	Enables an encryption method in the WPA authentication mode.
disable	Disables an encryption method in the WPA authentication mode.

【Default Configuration】 N/A

【Command Mode】 WLAN security configuration mode

【Default Level】 14

【Usage Guide】 This command is used to enable encryption in WPA authentication mode, there are two encryption methods: AES and TKIP. In a WLAN security configuration mode, both AES and TKIP encryption methods can be enabled at the same time.

【Configuration Example】 1: Configure the encryption method in WLAN 1 WPA authentication mode as AES.

```
AC-FS(config)#wlansec 1
AC-FS(config-wlansec)#security wpa enable
AC-FS(config-wlansec)#security wpa ciphers aes enable
```

【Verification】1: Use the show running-config command to check whether the configuration takes effect.

【Prompt Information】 1: If WPA authentication is not enabled in WLAN security configuration mode, an error will be displayed when configuring the encryption mode of WPA mode.

```
AC-FS(config)#wlansec 1
AC-FS(config-wlansec)#security wpa ciphers aes enable
WLAN 1 wpa is disable.
```

【Common Mistake】 1: In the WLAN security configuration mode, configure the WPA encryption method without enabling WPA authentication.

2: The WPA authentication is enabled in the WLAN security configuration mode, but the encryption mode is not configured, so that the terminal cannot associate with the wireless network.

【Platform Description】-

1.22 scurity wpa3 dot11r

Turn off the 802.11r functionality for the WPA3.

security wpa3 dot11r disable

Turn on the 802.11r function of the WPA3.

security wpa3 dot11r enable

【Parameter Description】

Parameter	Description
disable	Disable 802.11r feature of wpa3.
enable	Enable 802.11r function of wpa3.

【Default Configuration】 The 802.11r function of WPA3 is not turned on, with the disable status.

【Command Mode】 WLAN, security mode

【Default Level】 14

【Usage Guide】 Before enabling the 802.11r function, please select an effective mode of WPA3 through security wpa3 mode. Only the Personal or Enterprise mode is supported, and the Enhanced-Open mode does not support enabling 802.11r.

【Configuration Example】 Configure WLAN 1 to pure WPA3 Personal mode and turn 802.11r on.

```
AC-FS(config)#wlansec 1
AC-FS(config-wlansec)#security pmf optional AC-FS(config-
wlansec)#security wpa3 mode personal
AC-FS(config-wlansec)#security wpa3 dot11r enable
```

【Verification】 Use the show running-config command to see if the configuration takes effect.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.23 security wpa3 mode

Close WPA3.

security wpa3 mode none

Set the WPA3 to the Personal mode

security wpa3 mode personal

Set the WPA3 to the Enterprise mode.

security wpa3 mode enterprise

Set the WPA3 to the Enhanced Open mode

security wpa3 mode enhanced-open

【Parameter Description】

Parameter	Description
none	Turn off the WPS3.
personal	Select the WPA3 Personal mode that can be mixed with the WPA2 PSK.
enterprise	Select the WPA3 Enterprise mode.
enhanced-open	Select the WPA3 Enhanced Open mode.

【Default Configuration】 The WPA3 mode is none, that is, it is not on

【Command Mode】 The WLAN security configuration mode

【Default Level】 14

【Usage Guide】 This command can set the mode of WPA3, there are currently three modes to choose from: Personal, Enterprise and Enhanced-open. Since WPA3 relies on 802.11w, before setting these two modes of WPA3, you need to set pmf to optional or mandatory.

1. Personal mode before setting WPA3: it is pure WPA3 mode, because it is compatible with WPA2, it can also mix with WPA2 PSK, which does not allow TKIP encryption when mixing with WPA2 PSK.

2. Enterprise mode: Not compatible with WPA2, but only pure WPA3 Enterprise mode.

3. Enhanced-open mode: The user does not need to enter authentication information, but the associated data messages are encrypted.

None of the above modes are compatible with the WPA, and when enabled, clear the relevant settings for the WPA first.

【Configuration Example】1: Configure WLAN 1 as pure WPA3 Personal mode and the password is abc.

```
AC-FS(config)#wlansec 1
AC-FS(config-wlansec)#security pmf optional
AC-FS(config-wlansec)#security wpa3 personal passphrase abc
AC-FS(config-wlansec)#security wpa3 mode personal
```

2: Configure WLAN 1 to WPA3 Personal mode, password to abc, additionally mixed with the PSK of WPA2.If STA chooses to associate with WPA3 Personal, the password is abc, and if STA selects for association with WPA2 PSK, it is 123456789.

```
AC-FS(config)#wlansec 1
AC-FS(config-wlansec)#security pmf optional
AC-FS(config-wlansec)#security wpa3 personal passphrase abc
AC-FS(config-wlansec)#security wpa3 mode personal AC-
FS(config-wlansec)#security rsn enable
AC-FS(config-wlansec)#security rsn cipher aes enable
AC-FS(config-wlansec)#security rsn akm psk enable
AC-FS(config-wlansec)#security rsn akm psk set-key ascii 123456789
```

3: Configure the WLAN 1 to be in pure WPA3 Enterprise mode.

```
AC-FS(config)#wlansec 1
AC-FS(config-wlansec)#security pmf optional AC-
FS(config-wlansec)#security wpa3 mode enterprise
```

4: Configure the WLAN 1 to be in the WPA3 Enhanced Open mode.

```
AC-FS(config)#wlansec 1
AC-FS(config-wlansec)#security pmf mandatory AC-
FS(config-wlansec)#security wpa3 mode enhanced-open
```

【Verification】 Use the show running-config command to see if the configuration takes effect

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.24 security wpa3 personal passphrase ascii

Set the password for WPA3 to the Personal mode.

security wpa3 personal passphrase ascii ***password***

【Parameter Description】

Parameter	Description
password	ascii characters from 1 to 63 in length.

【Default Configuration】 No password.

【Command Mode】 The WLAN security configuration mode

【Default Level】 14

【Usage Guide】 This command sets the password for WPA3 Personal mode, which is used in pure WPA3 Personal mode, AP negotiation with STA. When mixing with the WPA2 PSK, this password is used if the STA supports the WPA3, and the password for the WPA2 PSK is not supported.

【Configuration Example】 The password for configuring the WLAN 1 WPA3 personal is abc

```
AC-FS(config)#wlansec 1
AC-FS(config-wlansec)#security wpa3 personal passphrase abc
```

【Verification】 Use the show running-config command to see if the configuration takes effect.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.25 security wpa3 personal passphrase none

Clear the password for the WPA3 Personal mode.

security wpa3 personal passphrase none

【Parameter Description】 -

【Default Configuration】 No password.

【Command Mode】 The WLAN security configuration mode

【Default Level】 14

【Usage Guide】 This command clears the password of WPA3 Personal mode. In pure WPA3 Personal mode, this password is used in the negotiation between AP and STA. Before clearing, it is necessary to cancel WPA3 Personal mode.

When mixing with WPA2 PSK, if the password of WPA3 Personal is cleared, when the STA associates, whether it supports WPA3 Personal or not, it will use the password of WPA2 PSK to associate.

【Configuration Example】 1: Clear the password of WLAN 1 WPA3 personal.

```
AC-FS(config)#wlansec 1
AC-FS(config-wlansec)#security wpa3 mode none
AC-FS(config-wlansec)#security wpa3 personal passphrase none
```

【Verification】 Use the show running-config command to see if the configuration takes effect.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.26 security wpa3 enhanced-open paired-wlan

Configure the equivalent WLAN for the WPA3 OWE mode.

security wpa3 enhanced-open paired-wlan ***wlanid***

Remove the equivalent WLAN of the WPA3 OWE mode.

security wpa3 enhanced-open paired-wlan none

【Parameter Description】

Parameter	Description
wlanid	Equivalent wlan id of the WPA3 OWE mode.
none	Clear out the equivalent WLAN.

【Default Configuration】 none

【Command Mode】 The WLAN security configuration mode

【Default Level】 14

【Usage Guide】 1. In scenarios with WPA3 OWE mode configured, mobile terminals that do not support OWE mode will not be successfully associated with WPA3 OWE mode signals. This problem can be solved by configuring an equivalent WLAN in WPA3 OWE mode on the device.

2. The valent WLAN must be pre-configured and wireless signal OPEN

3. The qos, schedule and other configurations of the equivalent WLAN must be consistent with the configuration of the WPA3 OWE signal.

4. he signal should be configured as hidden mode after config the equivalent WLAN of WPA3 OWE mode.

5. The WLAN of the same OPEN cannot act as an equivalent WLAN for 2 WPA3 OWE signals and more signals simultaneously.

【Configuration Example】 Create WLAN 1, configure WLAN 1 to be in WPA3 OWE mode, create WLAN 2, and configure WLAN 2 to be the equivalent to WLAN while hiding the WLAN 1 wireless signal.

```
AC-FS(config)#wlan-config 1 Open-USA-OWE
AC-FS(config-wlan)#exit AC-
FS(config)#wlan-config 2 Open-USA AC-
FS(config-wlan)#exit AC-FS(config)#wlansec
1
AC-FS(config-wlansec)#security pmf mandatory AC-
FS(config-wlansec)#security wpa3 mode enhanced-open
AC-FS(config-wlansec)#security wpa3 enhanced-open paired-wlan 2
AC-FS(config)#exit
AC-FS(config-wlan)#wlan-config 1
AC-FS(config)#no enable-broad-ssid
AC-FS(config)#exit
```

【Verification】 Use the show running-config command to see if the configuration takes effect.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.27 show wclient security

View the security configuration information for the STA

show wclient security *mac-address*

【Parameter Description】

Parameter	Description
mac-address	The MAC address of the STA want to view.

【Command Mode】 Privilege mode, global mode, WLAN security configuration mode

【Default Level】 1

【Usage Guide】 Use this command to see whether the STA authentication is complete, security policy, WPA version, unicast encryption suite, EAP type, and other informati

【Configuration Example】 View the security configuration information for the STA(3848.4c48.d953).

```
AC-FS# show wclient security 3848.4c48.d953
Security policy finished      :TRUE
Security policy type          :PSK
Security WPA version          :WPA2
Security Ucast cipher         :CCMP
Security EAP type             :NONE
```

【Field interpretation】

Field	Interpretation:
Security policy finished	Is the certification complete.
Security policy type	security policy.
Security WPA version	WPA version.
Security Ucast cipher	Single-broadcast encryption suite.
Security EAP type	EAP type.

【Prompt Information】 Error is prompted if no STA information is available on the device.

```
AC-FS#show wclient security 3848.4c48.d953
No station info for this MAC   :3848.4c48.d953
```

【Platform Description】 -

1.28 show wlan security

Displays the security configuration information for the WLAN

show wlan security *wlan-id*

【Parameter Description】

Parameter	Description
wlan-id	The ID of the WLAN that you want to view.

【Command Mode】 Privilege mode, global mode, WLAN security configuration mode

【Default Level】 1

【Usage Guide】 Use this command to view the security configuration information for WLAN, including WPA version, authentication mode, multicast encryption suite, multicast encryption suite, multicast key, and other information.

【Configuration Example】 1. View the security configuration information for the WLAN 1.

```
AC-FS#show  wlan  security  1
WLAN SSID           : AC-FS-psk
Security Policy  : PSK
WPA version         :  RSN(WPA2)
AKM type            : preshare key
pairwise cipher type: AES
group cipher type : AES
wpa_passphrase_len  : 8
wpa_passphrase      : 31 32 33 34 35 36 37 38
group key           : 39 de c7 57 5c 58 9a af 84 84 cf 18 3e ce ff 5c
```

2. View the security configuration information for the WLAN 2, and the WLAN is in WPA3 Enterprise mode.

```
AC-FS#show wlan security 2
WLAN SSID           : WPA3-ENTERPRISE-DEMO
Security Policy.....802.1X-WPA3
WPA version         :  WPA3
SAE                 : False
802.1X              :  True
PSK                 : False
pairwise cipher type: GCMP256
group cipher type : GCMP256
wpa_passhraselen : 0
wpa_passphrase      :
sae_passhraselen : 0
sae_passphrase      :
group key           : 8c cd b3 84 8f 33 a4 2d 51 73 02 94 1c da 34 c6 19 68 1e 8a 60 aa aa 0e 16
ec 89 9f 3f d1 9b fe
```

【Field interpretation】

Field	Interpretation
WLAN SSID	SSID of WLAN.
Security Policy	The WLAN security policy, added the following field, meaning as follows: SAE, indicating that it is pure WPA3 Pesonal=SAE/PSK, Represents the WPA3 Personal and the WPA2 PSK. The mixed mode of 802.1X-WPA3, indicating the WPA3 Enterprise.

WPA version	WPA version.
AKM type	AKM suite, access authentication.
pairwise cipher type	Spreading Key Kit.
group cipher type	Hoast the key suite.
wpa_passphrase_len	Configured password length.
wpa_passphrase	Configured PSK password.
group key	Multicast key for WLAN.

【Prompt Information】 An error is prompted if the corresponding WLAN does not have any security policies enabled.

```
AC-FS#show wlan security 2
No wlan config for this wlanid (2).
```

【Platform Description】 -

1.29 webauth prevent-jitter

Configure the WEB authentication stabilization time for WLAN

webauth prevent-jitter *timeout*

Remove the WEB authentication anti-shake time configuration

no webauth prevent-jitter

Restore the Default Configuration.

default webauth prevent-jitter

【Parameter Description】

Parameter	Description
timeout	Configure the WEB authentication anti-shake time, in seconds. The value range of timeout is 0s- - -86400s (timeout 0 means off WEB authentication anti-shake).

【Default Configuration】 WEB authentication anti-shake time, the default value is 300 seconds

【Command Mode】 The WLAN security configuration mode

【Default Level】 14

【Usage Guide】 This command is used to configure the WEB authentication antishake time in WLAN Security Configuration mode. The WEB authentication must be enabled before the WEB authentication stabilization time can be configured.

【Configuration Example】 The WEB authentication stabilization time for the configuration of the WLAN 1 is 900 seconds.

```
AC-FS(config)#wlansec 1
AC-FS(config-wlansec)#webauth
AC-FS(config-wlansec)#webauth prevent-jitter 900
```

【Verification】 Use the show running-config command to see if the configuration takes effect

【Prompt Information】 An error is prompted if the WEB authentication stabilization time parameter is configured if the WEB authentication is not enabled.

```
AC-FS(config-wlansec)#webauth prevent-jitter 900
Please config webauth first!
```

【Common Mistake】 Configure the WEB authentication stabilization time without WEB authentication is enabled.

【Platform Description】 -

1.30 wlansec

Enter the security configuration mode of the specified WLAN through the wlansec command

wlansec *wlan-id*

Remove the security configuration mode.

no wlansec *wlan-id*

Restore the Default Configuration.

default wlansec *wlan-id*

【Parameter Description】

Parameter	Description
wlan-id	Configure the ID of the WLAN.

【Default Configuration】 Security configuration mode for the WLAN, was not created

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Enter the security configuration mode for the specified WLAN, and the WLAN must have been created. Users can remove the security configuration of this WLAN with the no wlansec wlan-id command

【Configuration Example】 Configure the security configuration mode for creating the WLAN 1.

```
AC-FS(config)#wlansec 1
```

【Verification】 Use the show wlan security 1 command to see if the WLAN 1 security configuration mode was created successfully.

【Prompt Information】 An error is prompted if the WLAN for the configured security configuration mode is not created

```
AC-FS(config)#wlansec 2
AC-FS(config)#No wlan or no ssid for this wlanid(2).
```

【Common Mistake】 The WLAN intended to configure the security configuration mode is not created.

【Platform Description】 -

2 WIDS

2.1 attack-detection enable

Configure the detection type to enable the IDS attack detection function.

attack-detection enable { all | flood | ddos | spoof | weak-iv }

Configure the detection type to disable the IDS attack detection function.

no attack-detection enable { all | flood | ddos | spoof | weak-iv }

【Parameter Description】

Parameter	Description
all	Indicates all IDS attack detection types.
flood	Indicates the type of Flooding IDS attack detection.
ddos	Indicates the DDOS IDS attack detection type.
spoof	Indicates the Spoof IDS attack detection type.
weak-iv	Indicates the Weak-Iv attack detection type.

【Default Configuration】 It is closed by default.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 This command is used to enable the IDS attack detection function.

【Configuration Example]】1: Enable the Flooding IDS attack detection function.

```
AC-FS(config-wids)# attack-detection enable flood
```

2: Disable the flooding IDS attack detection function.

```
AC-FS(config-wids)#no attack-detection enable flood
```

【Verification】1: Use the show running-config command to view the IDS attack detection type configuration information

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.2 attack-detection ddos

Configure the detection threshold and cycle duration of specified types of ddos attacks

attack-detection ddos { arp-threshold num | icmp-threshold num | syn-threshold num | interval time }

Restores the specified type of packet threshold and period duration for ddos attacks to the default values.

no attack-detection ddos { arp-threshold | icmp-threshold | syn-threshold | interval }

【Parameter Description】

Parameter	Description
interval time	ddos detection period, the range is 10~60s.
arp-threshold num	arp packet threshold, the range is 1~10000pps.
icmp-threshold num	icmp message threshold, the range is 1~10000pps.
syn-threshold num	syn message threshold, the range is 1~10000pps.

【Default Configuration】 The default threshold for arp is 5pps, the default threshold for icmp is 100pps, the default threshold for syn is 5pps, and the default detection period for ddos is 30s.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the threshold for ddos attack arp packets to be 200pps.

AC-FS(config-wids)# attack-detection ddos arp-threshold 200

2: Restore the threshold value of the ddos attack arp packet to the default value.

AC-FS(config-wids)#no attack-detection ddos arp-threshold

【Verification】1: Use the show running-config command to view the threshold and cycle duration of various types of packets detected by ddos attacks.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.3 attack-detection flood multi-mac

Configure the threshold and cycle duration of specified types of packets for multi-user flood attacks.

attack-detection flood multi-mac { assoc | reassoc | disassoc | probe | action | auth | deauth |

null-data } threshold num interval time

Restore the specified type of packet threshold and cycle duration for multi-user flood attacks to the default values.

no attack-detection flood multi-mac { assoc | reassoc | disassoc | probe | action | auth | deauth | null-data }

【Parameter Description】

Parameter	Description
assoc	association message.
reassoc	reassocation message.
disassoc	disassociation message.
probe	probe request message.
action	action message.
auth	authentication message.
deauth	deauthentication message.
null-data	null data message.
threshold num	Attack packet threshold, the range is 1~5000.
interval time	Statistical period message threshold, the period is 10~60s.

【Default Configuration】 The default packet threshold for all flood attack detection is 500, and the default statistics period is 10s.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the assoc packet threshold for multi-user flood attack detection to be 200, and the statistical period to be 20000ms.

```
AC-FS(config-wids)# attack-detection flood multi-mac assoc threshld 200 interval 20000
```

2: Restore the assoc packet threshold and statistical period for multi-user flood attack detection to default values.

```
AC-FS(config-wids)#no attack-detection flood multi-mac assoc
```

【Verification】1: Use the show running-config command to configure the detection value of the packets of multi-user flood attack detection.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.4 attack-detection flood single-mac

Configure the threshold and cycle duration of a specified type of flood attack for a single-user user

attack-detection flood single-mac { total | assoc | reassoc | disassoc | probe | action | auth | deauth | null-data } threshold num interval time

Restores the specified type of packet threshold and cycle duration for a single-user flood attack to the default values.

no attack-detection flood single-mac { tota | assoc | reassoc | disassoc | probe | action | auth | deauth | null-data }

【Parameter Description】

Parameter	Description
total	all messages.
assoc	association message.
reassoc	reassocation message.
disassoc	disassociation message.
probe	probe request message.
action	action message.
auth	authentication message.
deauth	deauthentication message.
null-data	null data message.

threshold num	Attack packet threshold, the range is 1~5000.
interval time	Statistical period message threshold, the period is 10~60s.

【Default Configuration】 The default packet threshold for all flood attack detection is 300, and the default statistics period is 10s.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the assoc packet threshold for single-user flood attack detection to be 200, and the statistical period to be 20000ms.

```
AC-FS(config-wids)# attack-detection flood single-mac assoc threshld 200 interval 20000
```

2: Restore the asso packet threshold and statistical period for single-user flood attack detection to the default values.

```
AC-FS(config-wids)#no attack-detection flood single-mac assoc
```

【Verification】1: Use the show running-config command to configure the packet detection configuration value for single-user flood attack detection.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.5 attack-detection spoof

Configure the spoof attack packet threshold

attack-detection spoof { threshold num | interval time }

Restore the spoof attack packet threshold to the default value.

no attack-detection spoof { threshold | interval }

【Parameter Description】

Parameter	Description
threshold num	Packet threshold, the range is 1~1000
interval time	Detection cycle, the range is 10~60s

【Default Configuration】 The default packet threshold is 1, and the default detection period is 50s.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the threshold value of spoof attack packets to be 20.

```
AC-FS(config-wids)# attack-detection spoof threshold 20
```

2: Restore the threshold value of the spoof attack arp packet to the default value.

```
AC-FS(config-wids)#no attack-detection spoof threshold
```

【Verification】1: Use the show runnin-config command to view the detection configuration of various types of spoof attack packets.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.6 attack-detection weak-iv

Configure the packet detection threshold and period for weak-iv attacks.

attack-detection weak-iv { threshold num | interval time }

Restore the packet detection threshold and cycle duration for weak-iv attacks.

no attack-detection weak-iv { threshold | interval }

【Parameter Description】

Parameter	Description
threshold num	weak-iv detection packet threshold, the range is 1~10000.
interval time	weak-iv detection period duration, the range is 1~60s.

【Default Configuration】 The default threshold for weak-iv detection packets is 10, and the default detection period is 15s.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the weak-iv detection packet threshold to 200.

```
AC-FS(config-wids)# attack-detection weak-iv threshold 200
```

2: Restore the weak-iv detection packet threshold to the default value.

```
AC-FS(config-wids)#no attack-detection weak-iv threshold
```

【Verification】1: Use the show runnin-config command to view the packet detection configuration value and period of weak-iv

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.7 attack-detection statistics ac-max

Configure the length of the AC side of the IDS attack detection list.

attack-detection statistics ac-max num

Restore the length of the AC side of the IDS attack detection list to the default value.

no attack-detection statistics ac-max

【Parameter Description】

Parameter	Description
num	Indicates the limit of the number of ids attack detection list AC side, the range is 1~4096。

【Default Configuration】 The default value is 2048.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the length of the AC side of the IDS attack detection list to be 2000.

```
AC-FS(config-wids)# attack-detection statistics ac-max 2000
```

2: Restore the length of the AC side of the IDS attack detection list to the default value.

```
AC-FS(config-wids)#no attack-detection statistics ac-max
```

【Verification】1: Use the show runnin-config command to view the length of the AC side of the IDS attack detection list.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.8 attack-detection statistics ap-max

Configure the length of the AP side of the IDS attack detection list.

attack-detection statistics ap-max num

Restore the length of the AP side of the IDS attack detection list to the default value.

no attack-detection statistics ap-max

【Parameter Description】

Parameter	Description
num	Indicates the limit of the number of ids attack detection list on the AP side, the range is 1~1024。

【Default Configuration】 The default value is 512.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the length of the IDS attack detection list on the AP side to be 1000.

```
AC-FS(config-wids)# attack-detection statistics ap-max 1000
```

2: Restore the length of the AP side of the IDS attack detection list to the default value.

```
AC-FS(config-wids)#no attack-detection statistics ap-max
```

【Verification】1: Use the show running-config command to view the length of the AP side of the IDS attack detection list

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.9 countermeasures ap-max

Configure the maximum number of devices to be countered per device.

countermeasures ap-max ap-num

Restore the maximum number of devices to be countered each time to the default number.

no countermeasures ap-max

【Parameter Description】

Parameter	Description
ap-num	The maximum number of devices to be countered each time, the range is 1~256.

【Default Configuration】 The default number is 30.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 This command is used to configure the maximum number of devices to be countered each time. This function requires the device counter function to be enabled.

【Configuration Example]】1: The maximum number of devices that can be configured for device countermeasures is 22.

```
AC-FS(config-wids)# countermeasures ap-max 22
```

2: The maximum number of devices to be countered by the recovery device is the default value.

```
AC-FS(config-wids)#no countermeasures ap-max
```

【Verification】1: Use the show running-config command to view the maximum number of countermeasures each time

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.10 countermeasures enable

Configure to enable the device anti-counterfeiting function.

countermeasures enable

Configure to disable the device anti-counterfeiting function.

no countermeasures enable

【Parameter Description】–

【Default Configuration】 It is closed by default.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 This command is used to enable the device countermeasure function. The device countermeasure function does not take effect when the AP works in normal mode.

【Configuration Example】1: Enable the device counter function.

```
AC-FS(config-wids)#countermeasures enable
```

2: Turn off the device counter function.

```
AC-FS(config-wids)#no countermeasures enable
```

【Verification】1: Use the show running-config command to check whether the device counter function is enabled

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.11 countermeasures channel-match

The configuration enables channel-based countermeasures.

countermeasures channel-match

Configure to disable channel-based countermeasures.

no countermeasures channel-match

【Parameter Description】–

【Default Configuration】 It is closed by default.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 This command is used to configure the channel-based countermeasure function, which requires the device counter function to be enabled.

【Configuration Example】1: Enable the channel-based countermeasure function.

```
AC-FS(config-wids)# countermeasures channel-matah
```

2: Disable the channel-based countermeasure function.

```
AC-FS(config-wids)#no countermeasures channel-match
```

【Verification】1: Use the show running-config command to check the status of channel-based countermeasures.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.12 countermeasures interval

Configure the period for the device countermeasure function.

countermeasures interval time

The period for restoring the device countermeasure function is the default period.

no countermeasures interval

【Parameter Description】

Parameter	Description
time	The cycle duration of the device counter function, the range is 100~10000ms.

【Default Configuration】 The default duration of the countermeasure function is 1000ms.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 This command is used to configure the duration of the device counter function.

【Configuration Example】1: The duration of configuring the device counter function is 2000ms.

```
AC-FS(config-wids)# countermeasures interval 2000
```

2: The duration of restoring the device counter function is the default value.

```
AC-FS(config-wids)#no countermeasures interval
```

【Verification】1: Use the show running-config command to check the duration of the device's counter function.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.13 countermeasures mode

Configure to enable the device anti-counterfeiting function.

countermeasures mode { all | adhoc | config | rogue | ssid }

Configure to disable the device anti-counterfeiting function.

no countermeasures mode { all | adhoc | config | rogue | ssid }

【Parameter Description】

Parameter	Description
all	Indicates that all anti-modes are enabled.
adhoc	Indicates countermeasures against detected illegal adhoc devices.
config	Indicates the device in the anti-attack list entry or in the ssid blacklist.
rogue	Indicates an illegal ap device detected by the counter (the signal value exceeds the counter signal value).
ssid	Indicates to counter the detection device with the same ssid on the AP.

【Default Configuration】 It is closed by default.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 This command is used to configure the counter mode of the device, which is valid only when the counter function is enabled.

【Configuration Example】1: Turn on the device counter mode adhoc.

```
AC-FS(config-wids)#countermeasures mode adhoc
```

2: Disable the function that the device's anti-mode is adhoc.

```
AC-FS(config-wids)#no countermeasures mode adhoc
```

【Verification】1: Use the show running-config command to view the enabled device counter mode

【Prompt Information】 1: If the countermeasure function is not enabled and the countermeasure mode is configured, an error will be prompted.

```
Countermeasures has not been enabled!
```

【Common Mistake】-

【Platform Description】-

2.14 countermeasures rssi-min

Configure the lower limit of the counter signal strength for the counter function of the device.

countermeasures rssi-min num

Restore the lower limit of the counter signal strength of the counter function of the device to the default value.

no countermeasures rssi-min

【Parameter Description】

Parameter	Description
num	The lower limit of the counter signal strength of the device counter function, the range is 0~75(-95~-20).

【Default Configuration】 The lower limit of the counter signal strength of the default counter function is 25 (-70).

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 This command is used to configure the lower limit of the counter signal strength of the counter function of the device. When the counter function is not enabled, configuring this function is invalid.

【Configuration Example】1: The lower limit of the counter signal strength for configuring the counter function of the device is 40.

```
AC-FS(config-wids)# countermeasures rssi-min 40
```

2: Restore the lower limit of the counter signal strength of the device counter function to the default value.

```
AC-FS(config-wids)#no countermeasures rssi-min
```

【Verification】1: Use the show running-config command to view the lower limit of the counter signal strength of the counter function of the device

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.15 countermeasures fuzzy-enable

Configure the device to enable blurring.

countermeasures fuzzy-enable

Turn off the device blurring function.

no countermeasures fuzzy-enable

【Parameter Description】–

【Default Configuration】Close by default

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 This command is used to configure the fuzzy anti-counterfeiting function of the device, which supports fuzzy matching of the SSID of the rogue AP. When the anti-pattern mode includes the config mode, the anti-counter and the name in the SSID blacklist (device black-ssid ssidname) Similar rogue APs; when the counter mode includes ssid mode, counter the rogue APs with similar SSIDs to the local machine. Fuzzy countermeasures only take effect in config and ssid modes.

【Configuration Example]】1: Configure the device to enable fuzzy countermeasures.

```
AC-FS(config-wids)# countermeasures fuzzy-enable
```

2: Configure the device to turn off fuzzy countermeasures.

```
AC-FS(config-wids)#no countermeasures fuzzy-enable
```

【Verification】1: Use the show running-config command to check the status of the device's fuzzy anti-counterfeiting function.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.16 countermeasures fuzzy-keyword

Configure fuzzy anti-keywords.

countermeasures fuzzy-keyword string

Remove the fuzzy counter keyword.

no countermeasures fuzzy-keyword string

【Parameter Description】

Parameter	Description
string	The configured fuzzy anti-keyword string is case-insensitive and is uniformly stored in lowercase.

【Default Configuration】 None

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】The fuzzy countermeasure function needs to be enabled with the countermeasures fuzzy-enable command to take effect. When the countermeasure mode includes the ssid mode, the rogue AP whose SSID contains the configuration keyword is countered. It supports automatic case recognition, such as AC-FS. There are 2^6 all case combinations, and only one of them needs to be configured to identify APs whose SSID contains various case combinations of AC-FS, such as AC-FS, AC-FS, etc. The fuzzy counter keyword only takes effect in ssid mode.

【Configuration Example]】1: Configure fuzzy countermeasure keywords.

```
AC-FS(config)# wids
AC-FS(config-wids)# countermeasures fuzzy-keyword test
```

2: Remove the fuzzy counter keyword.

```
AC-FS(config)# wids
AC-FS(config-wids)#no countermeasures fuzzy-keyword test
```

【Verification】1: Use the show wids fuzzy-keyword command to view the configuration information of the fuzzy anti-keyword of the device

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.17 device aging duration

Configure the detected device timeout period.

device aging duration time

Restore the detected device timeout to the default value.

no device aging duration

【Parameter Description】

Parameter	Description
time	The detected device timeout time, the range is 500~5000s.

【Default Configuration】 The default detected device timeout time is 1200s.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 This command is used to configure the timeout period of the detected device.

【Configuration Example】1: Configure the detected device timeout time as 1000.

```
AC-FS(config-wids)# device aging duration 1000
```

2: Restore the detected device timeout time to the default value.

```
AC-FS(config-wids)#no device aging duration
```

【Verification】1: Use the show running-config command to check the timeout time of the detected device

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.18 device attack mac-address

Configure the static attack list entry list.

device attack mac-address H.H.H

Delete the static attack list entry list.

no device attack mac-address H.H.H

【Parameter Description】

Parameter	Description
H.H.H	The MAC address of the static attack list entry list, indicating that bssid is the static attack list entry MAC detection device will be countered in config mode.

【Default Configuration】 The default is empty.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 This command is used to configure the static attack list entry list, which is one of the strategies to counter the Rogue device.

【Configuration Example】1: Set the static attack source MAC address of the device as 0000.0000.0001.

```
AC-FS(config-wids)# device attack mac-address 0000.0000.0001
```

2: Delete the static attack attack list with the MAC address of 0000.0000.0001.

```
AC-FS(config-wids)#no device attack mac-address 0000.0000.0001
```

【Verification】1: Use the show wids attack-list command to view the list of items in the configured static attack list.

【Prompt Information】 1: If the allowed MAC is already in the allowed MAC list, there will be an error message.

The mac address has been permitted!

【Common Mistake】-

【Platform Description】-

2.19 device attack max

Configure the length of the static attack list.

device attack max num

Restore the static attack list length to the default value.

no device attack max

【Parameter Description】

Parameter	Description
num	The length of the static attack list, the range is 1~1024.

【Default Configuration】 The default value is 512.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-.

【Configuration Example]】1: Set the length of the static attack list to 900.

```
AC-FS(config-wids)# device attack max 900
```

2: Restore the static attack list length to 512.

```
AC-FS(config-wids)#no device attack max
```

【Verification】1: Use the show running-config command to view the length of the configured static attack list.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.20 device black-ssid

Configure SSID blacklist entries.

device black-ssid ssid

Clears the specified ssid of the SSID blacklist entry.

no device black-ssid ssid

【Parameter Description】

Parameter	Description
ssid	Configure the ssid as a blacklist, indicating that the detection device with the SSID of the ssid will be countered when the countermeasure mode is config.

【Default Configuration】 The default is empty.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 This command is used to configure ssid blacklist.

【Configuration Example]】1: Configure SSID: my-wlan blacklist SSID.

```
AC-FS(config-wids)# device black-ssid my-wlan
```

2: Remove SSID: my-wlan from the blacklist SSID list entry.

```
AC-FS(config-wids)#no device black-ssid my-wlan
```

【Verification】1: Use the show wids blacklist command to view the configured SSID blacklist information

【Prompt Information】 1: If the length of SSID exceeds 32, there will be an error message.

```
SSID not more than 32 characters!
```

【Common Mistake】-

【Platform Description】-

2.21 device channel-bind

Configure the specified radio to scan channel information.

device channel-bind radio radio-id { channel num | max-cycles value }

The configuration restores the specified radio scan channel to its default value.

no device channel-bind radio radio-id

【Parameter Description】

Parameter	Description
radio radio-id	Indicates the radio id value.
channel num	Indicates the channel value, the default is China channel enabled, the configurable range is 1~255.
max-cycles value	Indicates the number of scans, the default value is 10 times, the configurable range is 0~255.

【Default Configuration】 See Parameter Description for the default value.

【Command Mode】 AP configuration mode.

【Default Level】 14

【Usage Guide】 -

【Configuration Example】 1: Configure the scan times of the interworking scan channel to be 20.

```
AC-FS#configure AC-
FS(config)#ap-config ap1
AC-FS(config-ap)#device channel-bind radio 1 max-cycles 20
```

【Verification】 Use show ap-config running ap-name to view the interworking scan channel information of the specified AP.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

2.22 device detected-ap-max

Configure the maximum number of members in the scanned AP linked list.

device detected-ap-max num

Configure the maximum number of members in the recovery scan AP linked list as the default value.

no device detected-ap-max num

【Parameter Description】

Parameter	Description
detected-ap-max num	Indicates the upper limit of the number of scanned APs, the default is 2048.

【Default Configuration】 See Parameter Description for the default value.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 -

【Configuration Example]】 1: Configure the maximum number of AP detection linked lists to be 1000.

```
AC-FS#configure AC-
FS(config)#wids
AC-FS(config-wids)#device detected-ap-max 1000
```

【Verification】 View the configuration information through show running.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

2.23 device friendly-flags

Configure device friendly identification.

device friendly-flags value

Restore device friendly id to default.

no device friendly-flags

【Parameter Description】

Parameter	Description
value	Configured device friendly identification value, ranging from 1 to 4294967295.

【Default Configuration】 The default value is 0.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】By configuring the friendly identifier of the device, the AC/AP can identify the friendly AP. The default value is the random friendly identification value generated by AC/AP.

【Configuration Example]】1: Configure the device friendly ID as 4294967295.

```
AC-FS(config-wids)# device friendly-flags 4294967295
```

2: Restore the device friendly identification value to the default value.

```
AC-FS(config-wids)#no device friendly-flags
```

【Verification】1: Use the show running-config command to view the user-friendly identifier value.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.24 device max-black-ssid

Configure the length of the SSID blacklist list.

device max-black-ssid num

Restore the SSID blacklist length to the default value.

no device max-black-ssid

【Parameter Description】

Parameter	Description
num	SSID blacklist list length, the range is 1～1024.

【Default Configuration】 The default value is 512.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Set the length of the SSID blacklist to 900.

```
AC-FS(config-wids)# device max-black-ssid 900
```

2: Restore the length of the SSID blacklist to the default value.

```
AC-FS(config-wids)#no device max-black-ssid
```

【Verification】1: Use the show running-config command to check the length of the configured SSID blacklist.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.25 device mode

Configure the AP working mode.

device mode { hybrid | monitor | normal }

Configure the recovery AP working mode.

no countermeasures mode

【Parameter Description】

Parameter	Description
hybrid	Indicates a mixed mode, serving as both an access device and a monitoring device.
monitor	Indicates monitoring mode, only as monitoring equipment.
normal	Indicates normal mode, only as an access device.

【Default Configuration】 The default working mode is normal.

【Command Mode】 AP configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: The configuration working mode is hybrid.

```
AC-FS#configure
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)#ap-config ap1
AC-FS(config-ap)#device mode hybrid
```

【Verification】View the working mode of the specified AP through show ap-config running ap-name.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.26 device permit mac-address

Configure the list of allowed MAC list entries.

device permit mac-address H.H.H

Delete the list of allowed MAC list entries.

no device permit mac-address H.H.H

【Parameter Description】

Parameter	Description
H.H.H	Allow MAC address list entry list MAC address, indicating that bssid is the detection device in the allowed MAC address list is a legal device.

【Default Configuration】 The default is empty.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 This command is used to configure the list of allowed MAC list entries, which is one of the policies used to counter the Rogue device.

【Configuration Example]】1: Set the list of allowed MAC list entries with the MAC address of 0000.0000.0001.

```
AC-FS(config-wids)# device permit mac-address 0000.0000.0001
```

2: Delete the list of allowed MAC list entries with the MAC address of 0000.0000.0001.

```
AC-FS(config-wids)#no device permit mac-address 0000.0000.0001
```

【Verification】1: Run the show wids permitted mac-address command to view the configured list of permitted MAC list entries.

【Prompt Information】 1: If the allowed MAC is already in the attack statistics list, there will be an error message.

```
The mac address has been attacked!
```

【Common Mistake】-

【Platform Description】-

2.27 device permit mac-address max

Configure the allowed MAC list length.

device permit mac-address max num

Restore allowed MAC list length to default.

no device permit mac-address max

【Parameter Description】

Parameter	Description
num	Indicates the length of the allowed MAC list, range (1~2048).

【Default Configuration】 The default allowed MAC list length is 1024.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Set the allowed MAC list length to 1000.

```
AC-FS(config-wids)# device permit mac-address max 1000
```

2: Restore the allowed MAC list length to the default value.

```
AC-FS(config-wids)#no device permit mac-address max
```

【Verification】1: Use the show running-config command to view the length of the configured allowable MAC list.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.28 device permit ssid

Configure the list of allowed SSID list entries.

device permit ssid ssid

Delete the list of allowed SSID list entries.

no device permit ssid ssid

【Parameter Description】

Parameter	Description
ssid	Configure the ssid as a list of allowed SSID list entries.

【Default Configuration】 The default is empty.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 This command is used to configure the list of allowed SSID list entries, which is one of the countermeasures for the device.

【Configuration Example]】1: Configure SSID: my-wlan is a list of allowed SSIDs.

```
AC-FS(config-wids)# device permit ssid my-wlan
```

2: Remove SSID: my-wlan from the list of allowed SSID list entries.

```
AC-FS(config-wids)#no device permit ssid my-wlan
```

【Verification】1: Use the show wids permitted ssid command to view the configured permitted SSID information

【Prompt Information】1: If the length of the configured ssid exceeds 32, it will prompt a configuration error

```
SSID not more than 32 characters!
```

【Common Mistake】-

【Platform Description】-

2.29 device permit max-ssid

Configure the allowed SSID list length.

device permit max-ssid num

Restore allowed SSID list length.

no device permit max-ssid

【Parameter Description】

Parameter	Description
num	Allowed SSID list length, range 1～1024.

【Default Configuration】 The default value is 512.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Set the allowed SSID list length to 900.

```
AC-FS(config-wids)# device permit max-ssid 900
```

2: Restore the allowed SSID list length to the default value.

```
AC-FS(config-wids)#no device permit max-ssid
```

【Verification】1: Use the show running-config command to view the length of the configured allowed SSID list.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.30 device permit vendor bssid

Configure the list of allowed manufacturer list entries.

device permit vendor bssid H.H.H

Delete the list of allowed manufacturers list entries.

no device permit vendor bssid H.H.H

【Parameter Description】

Parameter	Description
H.H.H	Allow Manufacturer MAC Address.

【Default Configuration】 The default is empty.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 The manufacturer number is the first 3 bytes of the MAC address. It is not allowed to configure multiple MAC addresses of the same manufacturer. This configuration is one of the strategies used to counter Rogue devices.

【Configuration Example]】1: Set the allowed manufacturer list entry with the MAC address of 0000.0000.0001.

```
AC-FS(config-wids)# device permit vendor bssid 0000.0000.0001
```

2: Delete the list of allowed manufacturers with the MAC address of 0000.0000.0001.

```
AC-FS(config-wids)#no device permit vendor bssid 0000.0000.0001
```

【Verification】1: Use the show wids permitted vendor command to view the configured list of permitted vendors

【Prompt Information】 1: If the manufacturer is allowed to repeat the configuration, there will be an error prompt.

```
The permitted vendor[vendor-mac] already exists!
```

【Common Mistake】-

【Platform Description】-

2.31 device permit vendor bssid max

Configure the allowable vendor list length.

device permit vendor bssid max num

Restore the allowable vendor list length to the default value.

no device permit vendor bssid max

【Parameter Description】

Parameter	Description
num	Indicates the allowable manufacturer list length, range (1~1024).

【Default Configuration】 The default allowable manufacturer list length is 512.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Set the allowable manufacturer list length to 1000.

```
AC-FS(config-wids)# device permit vendor bssid max 1000
```

2: Restore the allowable manufacturer list length to the default value.

```
AC-FS(config-wids)#no device permit vendor bssid max
```

【Verification】1: Use the show running-config command to view the length of the configured list of allowed manufacturers.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.32 device scan-para

Configure the scanning parameter for detecting illegal APs in interworking.

device scan-para { radio radio-id scan-type { active | passive } device-detect { enable | disable } |

ap-mode { normal | monitor } | detect-rpt-time time }

Configure the Detecting and Scanning Parameter for Restoring Interworking Rogue APs to the default values.

no device scan-para { radio radio-id | ap-mode | detect-rpt-time }

【Parameter Description】

Parameter	Description
radio radio-id	Indicates the radio value.
scan-type active	Indicates the scan type, active scan, default passive scan.
scan-type passive	Indicates the scan type, passive scan.
device-detect enable	Indicates detection is enabled, default is disabled.
device-detect disable	Indicates detection is off.
ap-mode normal	Indicates AP operation mode: normal mode.
ap-mode monitor	Indicates AP operating mode: Monitor Mode.
detect-rpt-time time	Indicates the detection reporting period, the default is 60s, the configurable range is 60~120s.

【Default Configuration】 See Parameter Description for default.

【Command Mode】 AP configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure and restore the interworking AP scan type and scan switch of the specified radio: 1 to the default values.

```
AC-FS#configure
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)#ap-config ap1
AC-FS(config-ap)#no device scan-para radio 1
```

【Verification】Use show ap-config running ap-name to view the scan information of the specified interworking AP.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.33 device unknown-sta dynamic-enable

Configure and enable the dynamic unknown name STA detection function.

device unknown-sta dynamic-enable

Configure to disable the dynamic unknown name STA detection function.

no device unknown-sta dynamic-enable

【Parameter Description】–

【Default Configuration】 It is closed by default.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 This function is only valid when the AP works in non-normal mode.

【Configuration Example]】1: Configure to enable dynamic unknown STA detection function.

```
AC-FS(config-wids)# device unknown-sta dynamic-enable
```

2: Configure to disable the dynamic unknown name STA detection function.

```
AC-FS(config-wids)#no device unknown-sta dynamic-enable
```

【Verification】1: Use the show running-config command to view the dynamic unknown name STA detection configuration

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.34 device unknown-sta mac-address

Configure the list of static unknown STA list entries.

device unknown-sta mac-address H.H.H

Delete the list of static unknown STA list entries.

no device unknown-sta mac-address H.H.H

【Parameter Description】

Parameter	Description
H.H.H	Indicates that the user with this MAC address is an unknown STA.

【Default Configuration】 The default is empty.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 This command is used to configure a static unknown STA list entry list, which is used to counter the policy of unknown STA devices.

【Configuration Example]】1: Set the device whose MAC address is 0000.0000.0001 as an unknown STA.

```
AC-FS(config-wids)# device unknown-sta mac-address 0000.0000.0001
```

2: Delete the unknown STA with the MAC address of 0000.0000.0001.

```
AC-FS(config-wids)#no device unknown-sta mac-address 0000.0000.0001
```

【Verification】1: Use the show wids unknown-sta command to view the information on the configured unknown name STA list entry list

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.35 device unknown-sta mac-address max

Configure the length of the unknown STA list.

device unknown-sta mac-address max num

Restore the length of the unknown STA list to the default value.

no device unknown-sta mac-address max

【Parameter Description】

Parameter	Description
num	Unknown name STA list length, range (1~256).

【Default Configuration】 The default unknown name STA list length is 128.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Set the length of the unknown STA list to 200.

```
AC-FS(config-wids)# device unknown-sta mac-address max 200
```

2: Restore the length of the unknown STA list to the default value.

```
AC-FS(config-wids)#no device unknown-sta mac-address max
```

【Verification】1: Use the show running-config command to check the length of the configured unknown STA list.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.36 device unknown-sta report enable

Configure and enable the function of reporting dynamic unknown STA detection information.

device unknown-sta report enable

Configure to disable the dynamic unknown name STA detection and reporting function.

no device unknown-sta report enable

【Parameter Description】–

【Default Configuration】 It is closed by default.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 This function is only valid when the AP works in non-normal mode, and the scanning results can be reported to the AC for data presentation.

【Configuration Example]】1: Configure to enable dynamic unknown STA detection and reporting function.

```
AC-FS(config-wids)# device unknown-sta report enable
```

2: Configure to disable the dynamic unknown name STA detection and reporting function.

```
AC-FS(config-wids)#no device unknown-sta report enable
```

【Verification】1: Use the show running-config command to view the configuration of the dynamic unknown name STA detection and reporting function

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.37 dos-detection

Configure the interworking anti-DOS attack detection function or the interworking anti-DOS attack related threshold information.

dos-detection { enable | threshold num | interval time }

The configuration restores interworking anti-DOS attack detection to the default value.

no dos-detection { enable | threshold | interval }

【Parameter Description】

Parameter	Description
enable	Indicates the interworking anti-DOS attack detection switch.
threshold num	Indicates the interworking anti-DOS attack detection packet threshold, ranging from 1 to 5000.
time	Indicates the interworking anti-dos attack detection cycle duration 1~60000ms.

【Default Configuration】 By default, the interworking anti-DOS attack function is disabled, the default anti-DOS attack detection packet threshold is 30, and the default anti-DOS attack detection cycle time is 1000ms.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Enable the interworking anti-DOS attack function.

```
AC-FS(config-wids)#dos-detection enable
```

【Verification】1: Use the show running-config command to view the configuration related to the interworking anti-DOS attack function.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.38 dynamic-blacklist enable

Configure to enable the dynamic blacklist function.

dynamic-blacklist enable

Configure to disable the dynamic blacklist function.

no dynamic-blacklist enable

【Parameter Description】–

【Default Configuration】 It is closed by default.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Enable the dynamic blacklist function.

```
AC-FS(config-wids)# dynamic-blacklist enable
```

2: Disable the dynamic blacklist function.

```
AC-FS(config-wids)#no dynamic-blacklist enable
```

【Verification】1: Use the show running-config command to check the status of the dynamic blacklist function.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.39 dynamic-blacklist lifetime

Configure the dynamic blacklist lifetime.

dynamic-blacklist lifetime time

Restore the dynamic blacklist lifetime to the default value.

no dynamic-blacklist lifetime

【Parameter Description】

Parameter	Description

time	The lifetime of the dynamic blacklist, the range is 60~86400s.

【Default Configuration】 The default dynamic blacklist lifetime is 300s.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the lifetime of the dynamic blacklist to be 600s.

```
AC-FS(config-wids)# dynamic-blacklist lifetime 600
```

2: Restore the dynamic blacklist lifetime to the default value.

```
AC-FS(config-wids)#no dynamic-blacklist lifetime
```

【Verification】1: Use the show running-config command to check the lifetime of the dynamic blacklist

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.40 dynamic-blacklist ac-max

Configure the length of the dynamic blacklist list on the AC side.

dynamic-blacklist ac-max num

Restore the length of the dynamic blacklist list on the AC side to the default value.

no dynamic-blacklist ac-max

【Parameter Description】

Parameter	Description
num	AC side dynamic blacklist list AC side length, the range is 1～4096.

【Default Configuration】 The default value is 2048.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Set the length of the dynamic blacklist list on the AC side to 2000.

```
AC-FS(config-wids)# dynamic-blacklist ac-max 2000
```

2: Restore the length of the dynamic blacklist list on the AC side to the default value.

```
AC-FS(config-wids)#no dynamic-blacklist ac-max
```

【Verification】1: Use the show running-config command to view the length of the configured dynamic blacklist list on the AC side.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.41 dynamic-blacklist ap-max

Configure the length of the dynamic blacklist list on the AP side.

dynamic-blacklist ap-max num

Restore the AP-side dynamic blacklist length to the default value.

no dynamic-blacklist ap-max

【Parameter Description】

Parameter	Description
num	The length of the dynamic blacklist list on the AP side, the range is 1 to 4096.

【Default Configuration】 The default value is 2048.

【Command Mode】 WIDS configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Set the AP-side dynamic blacklist length to 1000.

```
AC-FS(config-wids)# dynamic-blacklist ap-max 1000
```

2: Restore the AP-side dynamic blacklist length to the default value.

```
AC-FS(config-wids)#no dynamic-blacklist ap-max
```

【Verification】1: Use the show running-config command to view the length of the configured AP dynamic blacklist list.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.42 dynamic-blacklist mac-address

Configure the dynamic blacklist entry list.

dynamic-blacklist mac-address H.H.H

Delete the dynamic blacklist STA list entry list.

no dynamic-blacklist mac-address H.H.H

【Parameter Description】

Parameter	Description
H.H.H	Indicates that the user with this MAC address is on the dynamic blacklist.

【Default Configuration】 The default is empty.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 This command is used to configure the dynamic blacklist entry list, which is used to dynamically control the STA access and communication policy.

【Configuration Example】1: Set the device whose MAC address is 0000.0000.0001 as a dynamic blacklist.

```
AC-FS(config-wids)#dynamic-blacklist mac-address 0000.0000.0001
```

2: Delete the dynamic blacklist with the MAC address of 0000.0000.0001.

```
AC-FS(config-wids)#no dynamic-blacklist mac-address 0000.0000.0001
```

【Verification】1: Use the show wids blacklist dynamic command to view the list information of the configured unknown name STA list entries

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.43 hybrid-scan radio

Configure to enable radio scan switch status information.

hybrid-scan radio num enable

Configure to turn off the radio scan switch off state information.

hybrid-scan radio num disable

【Parameter Description】

Parameter	Description
radio num	Indicates the specified radio, enabled by default.

【Default Configuration】 See Parameter Description for the default value.

【Command Mode】 AP configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Configure to close the scanning of radio1.

```
AC-FS#configure AC-
FS(config)#ap-config ap1
AC-FS(config-ap)#hybrid-scan radio 1 disable
```

【Verification】View the scan channel configuration information of the specified AP through show ap-config running ap-name.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.44 kickout client

Configure to remove the current associated user.

kickout client H.H.H

【Parameter Description】

Parameter	Description
H.H.H	Remove the user's MAC address.

【Default Configuration】 The default is empty.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 This command is used to release the associated STA. Through this command, the association of the specified STA can be disconnected

【Configuration Example]】1: Configure to exclude users whose MAC address is 0000.0000.0001.

```
AC-FS(config-wids)# kickout client 0000.0000.0001
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.45 kickout threshold

Configure the low-speed user filtering threshold.

kickout threshold rate

Disable low-speed user filtering.

no kickout threshold

【Parameter Description】

Parameter	Description
rate	Packet sending and receiving rate, range 0~130Mbps

【Default Configuration】 By default, low-speed users are not filtered, and the rate threshold is 0.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 When the rate of the STA is lower than the specified threshold, the AP will disconnect the STA.

【Configuration Example】1: Configure the low-speed user filtering threshold to 20Mbps.

```
AC-FS(config-wids)# kickout threshold 20
```

2: Disable low-speed user filtering.

```
AC-FS(config-wids)#no kickout threshold
```

【Verification】1: Use the show running-config command to view the filtering threshold of low-speed users.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.46 reset attack-list all

Configure to clear the configuration information of static attack list entries.

reset attack-list all

【Parameter Description】–

【Default Configuration】 None.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 This command is used to clear the configuration information of static attack list entries.

【Configuration Example]】1: Clear the static attack list entry configuration information.

```
AC-FS(config-wids)#reset attack-list all
```

【Verification】1: Use the command show wids attacklist to check whether the clearing is successful.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.47 reset black-ssid all

Configure to clear the SSID blacklist entry configuration information.

reset black-ssid all

【Parameter Description】–

【Default Configuration】 None.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 This command is used to clear the configuration information of SSID blacklist entries.

【Configuration Example]】1: Clear the SSID blacklist entry configuration information.

```
AC-FS(config-wids)#reset black-ssid all
```

【Verification】1: Use show wids black-ssid to check whether the clearing is successful.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.48 reset detected

The configuration clears the detected device information of the specified type.

reset detected { all | adhoc | rogue { ap | client } | mac-address H.H.H }

【Parameter Description】

Parameter	Description
all	Indicates to clear all detected devices.
adhoc	Indicates to clear detected adhoc devices.
rogue ap	Indicates to clear the detected rogue ap device.
rogue client	Indicates that the detected rogue client device is cleared.
mac-address H.H.H	Indicates the MAC address of the device that needs to be cleared.

【Default Configuration】 None.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 None

【Configuration Example]】1: Clear the detected rogue ap information

```
AC-FS(config-wids)#reset detected rogue ap
```

2: Clear device detection information with MAC address 0000.0000.0001

```
AC-FS(config-wids)#reset detected mac-address 0000.0000.0001
```

【Verification】Use the command show wids detected to check whether it has been cleared.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.49 reset dos-detected

Configure to clear the information detected by interworking anti-DOS attack.

reset dos-detected

【Parameter Description】–

【Default Configuration】 None.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 None

【Configuration Example]】1: Clear the information detected by the interworking anti-DOS attack

```
AC-FS(config-wids)#reset dos-detected
```

【Verification】Use the command show wids dos-detected to check whether it has been cleared.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.50 reset dynamic-blacklist

Configure to clear dynamic blacklist entry information.

reset dynamic-blacklist { all | mac-address H.H.H }

【Parameter Description】

Parameter	Description
all	Indicates that all dynamic blacklist entries are cleared.
mac-address H.H.H	Indicates to clear the dynamic blacklist entries whose source MAC is H.H.H.

【Default Configuration】 None.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Clear the dynamic blacklist entry whose source MAC is 0000.0000.0001.

```
AC-FS(config-wids)# reset dynamic-blacklist mac-addres 0000.0000.0001
```

【Verification】Use the command show wids blacklist dynamic to check whether it has been cleared.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.51 reset fuzzy-keyword all

Clear the fuzzy counter keyword configuration.

reset fuzzy-keyword all

【Parameter Description】–

【Default Configuration】 None.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Clear the fuzzy counter keyword configuration.

```
AC-FS(config)# wids
AC-FS(config-wids)# reset fuzzy-keyword all
```

【Verification】Run the show wids fuzzy-keyword command to check whether it has been cleared.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.52 reset permit-mac all

The configuration clears the configuration information of the allowed MAC list entries.

reset permit-mac all

【Parameter Description】–

【Default Configuration】 None.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Clear the configuration information of the allowed MAC list entry.

```
AC-FS(config-wids)#reset permit-mac all
```

【Verification】Use the command show wids permitted mac-address to check whether it has been cleared.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.53 reset permit-ssid all

The configuration clears the configuration information of the allowed SSID list entry.

reset permit-ssid all

【Parameter Description】–

【Default Configuration】 None.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Clear the configuration information of the allowed SSID list entry.

```
AC-FS(config-wids)#reset permit-ssid all
```

【Verification】Use the command show wids permitted ssid to check whether the clearance has been successfully completed.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.54 reset permit-vendor all

The configuration clear allows the configuration information of the manufacturer list entry.

reset permit-vendor all

【Parameter Description】–

【Default Configuration】 None.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Clear the configuration information of the list of allowed manufacturers.

```
AC-FS(config-wids)#reset permit-vendor all
```

【Verification】Use the command show wids permitted vendor to check whether the clearance has been successfully completed.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.55 reset rogue-ap detected

Configure to clear the information detected by illegal APs in interworking.

reset rogue-ap detected

【Parameter Description】–

【Default Configuration】 None.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 None

【Configuration Example】1: Clear the communication detected by the illegal AP

```
AC-FS(config-wids)#reset rogue-ap detected
```

【Verification】Use the command show wids rogue-ap detected to check whether it has been cleared.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.56 reset ssid-filter

Configure to clear all or specify the blacklist and whitelist configuration information of the SSID.

reset ssid-filter { ssid all | in-ssid ssid }

【Parameter Description】–

【Default Configuration】 None.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Clear all SSID-based blacklist and whitelist configuration information.

```
AC-FS(config-wids)#reset ssid-filter ssid all
```

【Verification】Use the command show wids ssid-filter to check whether it has been cleared.

【Prompt Information】 1: If the specified SSID does not exist, there will be an error prompt.

```
There is no SSID[ssid] to filter!
```

【Common Mistake】-

【Platform Description】-

2.57 reset ssid-filter blacklist all

Configure to clear all SSID-based blacklist and whitelist blacklist configuration information.

reset ssid-filter blacklist all

【Parameter Description】–

【Default Configuration】 None.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Clear all SSID-based blacklist and whitelist blacklist configuration information.

```
AC-FS(config-wids)#reset ssid-filter blacklist all
```

【Verification】Use the command show wids ssid-filter blacklist all to check whether it has been cleared.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.58 reset ssid-filter blacklist all in-ssid

Configure to clear all blacklist configuration information based on the specified SSID.

reset ssid-filter blacklist all in-ssid string

【Parameter Description】

Parameter	Description
string	means clear all blacklist information based on SSID:string.

【Default Configuration】 None.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Clear all blacklist configuration information based on SSID:my-wlan.

```
AC-FS(config-wids)#reset ssid-filter blacklist all in-ssid my-wlan
```

【Verification】Use the command show wids ssid-filter blacklist all in-ssid string to check whether it has been cleared.

【Prompt Information】 1: If the SSID does not exist, there will be an error message.

```
There is no SSID[ssid] to filter!
```

【Common Mistake】-

【Platform Description】-

2.59 reset ssid-filter whitelist all

Configure to clear all SSID-based blacklist and whitelist configuration information.

reset ssid-filter whitelist all

【Parameter Description】–

【Default Configuration】 None.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Clear all SSID-based blacklist and whitelist configuration information.

```
AC-FS(config-wids)#reset ssid-filter whitelist all
```

【Verification】Use the command show wids ssid-filter whitelist all to check whether it has been cleared.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.60 reset ssid-filter whitelist all in-ssid

The configuration clears all whitelist configuration information based on the specified SSID.

reset ssid-filter whitelist all in-ssid string

【Parameter Description】

Parameter	Description
string	Indicates clear based on all whitelist information under SSID:string.

【Default Configuration】 None.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Clear all whitelist configuration information based on SSID:my-wlan.

```
AC-FS(config-wids)#reset ssid-filter whitelist all in-ssid my-wlan
```

【Verification】Use the command show wids ssid-filter whitelist all in-ssid string to check whether it has been cleared.

【Prompt Information】 1: If the SSID does not exist, there will be an error message.

```
There is no SSID[ssid] to filter!
```

【Common Mistake】-

【Platform Description】-

2.61 reset static-blacklist all

Configure to clear the configuration information of static blacklist entries.

reset static-blacklist all

【Parameter Description】–

【Default Configuration】 None.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Clear the static blacklist entry configuration information.

```
AC-FS(config-wids)# reset static-blacklist all
```

【Verification】Use the command show wids blacklist static to check whether it has been cleared.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.62 reset statistic all

Configure the detection information of clearing attack statistics list entries.

reset statistic all

【Parameter Description】–

【Default Configuration】 None.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Clear the attack statistics list entry detection information.

```
AC-FS(config-wids)# reset statistic all
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.63 reset unknown-sta all

Configure to clear the information of unknown STA list entries.

reset unknown-sta all

【Parameter Description】–

【Default Configuration】 None.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Clear the unknown name STA list entry information.

```
AC-FS(config-wids)#reset unknown-sta all
```

【Verification】Use the command show wids unknown-sta to check whether it has been cleared.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.64 reset user-isolation-permit-list all

Configure to clear the configuration information of user isolation allow list entries.

reset user-isolation-permit-list all

【Parameter Description】–

【Default Configuration】 None.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Clear the user isolation allow list entry information.

```
AC-FS(config-wids)#reset user-isolation-permit-list all
```

【Verification】Use the command show wids user-isolation permit-mac to check whether it has been cleared.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.65 reset whitelist all

Configure the configuration information of clear list list entries.

reset whitelist all

【Parameter Description】–

【Default Configuration】 None.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Clear the configuration information of the list list entry.

```
AC-FS(config-wids)#reset whitelist all
```

【Verification】Use the command show wids whitelist to check whether it has been cleared.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.66 rogue-ap countermeasures enable

Configure to enable the anti-interference function of illegal APs.

rogue-ap countermeasures enable

Configure to disable the anti-interference function of illegal APs.

no rogue-ap countermeasures enable

【Parameter Description】–

【Default Configuration】 It is closed by default.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Enable the anti-interworking function of illegal APs.

```
AC-FS(config-wids)#rogue-ap countermeasures enable
```

2: Disable the counter function of interworking illegal APs.

```
AC-FS(config-wids)#no rogue-ap countermeasures enable
```

【Verification】1: Use the show running-config command to view the configuration of the intercommunication countermeasure function.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.67 scan-channels { 802.11a | 802.11b } channels

Configure scan channels.

scan-channels { 802.11a | 802.11b } channels nuim1 num2…num13

Configure the recovery scan channel to default.

no scan-channels { 802.11a | 802.11b }

【Parameter Description】

Parameter	Description
802.11a	Indicates that the 5G channel is configured, and the default scan channel is empty.
802.11b	Indicates that the 2.4G channel is configured, and the default scan channel is empty.
channels num	Indicates the configured channel value.

【Default Configuration】 See Parameter Description for the default value.

【Command Mode】 AP configuration mode.

【Default Level】 14

【Usage Guide】 -

【Configuration Example】 1: Configure 5g scan channel 149 153 157.

```
AC-FS#configure AC-
FS(config)#ap-config ap1
AC-FS(config-ap)#scan-channels 802.11a channels 149 153 157
```

【Verification】 View the scan channel configuration information of the specified AP through show ap-config running ap-name.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

2.68 scan-channels dual-band

Configure automatic switching of frequency band scanning.

scan-channels dual-band radio radio-id

The configuration restores the automatic switching frequency band to the default value.

no scan-channels dual-band radio radio-id

【Parameter Description】

Parameter	Description
radio-id	Indicates the radio id value.

【Default Configuration】 By default, dual-frequency scanning is not enabled.

【Command Mode】 AP configuration mode.

【Default Level】 14

【Usage Guide】 The radio frequency of some AP products supports both 2.4G and 5G. When the radio frequency is used for scanning, you can use this command to automatically switch between the two frequency bands, and then obtain the scanning results of the two frequency bands and perform countermeasures. After switching the frequency band, scan the channel list configured for scan-channels { 802.11a | 802.11b } channels . In particular, for some AP products, there are channel restrictions, and scanning channels will automatically skip the restricted channels.

【Configuration Example】 1: Configure the third frequency of AP1 for dual frequency switching.

```
AC-FS#configure AC-
FS(config)#ap-config ap1
AC-FS(config-ap)# scan-channels dual-band radio 3
```

【Verification】 View the scan channel configuration information of the specified AP through show ap-config running ap-name.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】-

2.69 show wids attacklist

Displays the configuration information of static attack list entries of WIDS.

show wids attack-list

【Parameter Description】–

【Command Mode】 Privileged mode.

【Default Level】1

【Usage Guide】-

【Configuration Example]】1: Display the configuration information of static list entries of WIDS.

```
AC-FS# show wids attack-list
```

【Prompt Information】-

【Platform Description】-

2.70 show wids blacklist

Display the dynamic/static blacklist entry information of WIDS.

show wids blacklist { dynamic | static }

【Parameter Description】

Parameter	Description
dynamic	Indicates that the dynamic blacklist entry information is displayed.
static	Indicates that the static blacklist entry information is displayed.

【Command Mode】 Privileged mode.

【Default Level】1

【Usage Guide】-

【Configuration Example]】1: Display the static blacklist entry information of WIDS.

```
AC-FS# show wids blacklist static
```

2: Display the dynamic blacklist entry information of WIDS.

```
AC-FS# show wids blacklist dynamic
```

【Prompt Information】-

【Platform Description】-

2.71 show wids black-ssid

Display the SSID blacklist entry configuration information of WIDS.

show wids black-ssid

【Parameter Description】–

【Command Mode】 Privileged mode.

【Default Level】1

【Usage Guide】-

【Configuration Example]】1: Display the SSID blacklist entry configuration information of WIDS.

```
AC-FS# show wids black-ssid
```

【Prompt Information】-

【Platform Description】-

2.72 show wids detected

Displays information about the specified type of device detected by WIDS.

show wids detected { adhoc | all | friendly ap | interfering ap | rogue { adhoc-ap | ap | client | config-ap |

ssid-ap } | mac-address H.H.H }

【Parameter Description】

Parameter	Description
adhoc	Indicates that the detected adhoc networks are displayed.
all	Indicates that all WLAN detected devices are displayed.
friendly ap	Indicates that the detected friendly APs are displayed.
interfering ap	Indicates that the detected interfering APs are displayed.
rogue adhoc-ap	Indicates that an anti-pattern adhoc compliant device was detected.
rogue ap	Indicates that a device compliant with the anti-mode rogue was detected.
rogue client	Indicates that the detected Rogue client devices are displayed.
rogue config-ap	Indicates to display detected devices conforming to the anti-pattern config.
rogue ssid-ap	Indicates to display detected devices compliant with the anti-pattern ssid.
mac-address H.H.H	Indicates that the detected devices whose source MAC is H.H.H are displayed.

【Command Mode】 Privileged mode.

【Default Level】1

【Usage Guide】-

【Configuration Example】1: Display the detected Rogue AP device information.

```
AC-FS# show wids detected rogue ap
```

【Prompt Information】-

【Platform Description】-

2.73 show wids dos-detected

Displays the intercommunication anti-DOS attack detection information.

show wids dos-detected

【Parameter Description】–

【Command Mode】 Privileged mode.

【Default Level】1

【Usage Guide】-

【Configuration Example]】1: Display the interworking anti-DOS attack detection information.

```
AC-FS# show wids dos-detected
```

【Prompt Information】-

【Platform Description】-

2.74 show wids fuzzy-keyword

Displays fuzzy counter keyword configuration information.

show wids fuzzy-keyword

【Parameter Description】–

【Command Mode】 Privileged mode.

【Default Level】1

【Usage Guide】-

【Configuration Example]】1: Display the configuration information of fuzzy countermeasure keywords.

```
AC-FS# show wids fuzzy-keyword
```

【Prompt Information】-

【Platform Description】-

2.75 show wids ssid-filter

Displays the configuration information of SSID-based black and white list entries.

show wids ssid-filter { blacklist all [in-ssid string] | ssid all | whitelist all [in-ssid string] }

【Parameter Description】

Parameter	Description
blacklist all	Indicates that all SSID-based blacklist entry information is displayed.
blacklist all in-ssid string	Indicates that all SSID-based blacklist entry information of the specified SSID is displayed.
ssid all	Indicates to display all SSID-based blacklist and whitelist SSID information.
whitelist all	Indicates that all SSID-based whitelist entry information is displayed.
whitelist all in-ssid string	Indicates that all SSID-based whitelist entry information of the specified SSID is displayed.

【Command Mode】 Privileged mode.

【Default Level】1

【Usage Guide】-

【Configuration Example]】1: Display all SSID-based blacklist entry information of WIDS

```
AC-FS# show wids ssid-filter blacklist all
```

【Prompt Information】-

【Platform Description】-

2.76 show wids permitted

Displays the configuration information of WIDS's allowed MAC, allowed SSID and allowed vendor list entries.

show wids permitted { mac-address | ssid | vendor }

【Parameter Description】

Parameter	Description
mac-address	Indicates the information of the allowed MAC address list entries.
ssid	Indicates the allowed SSID list entry information.
vendor	Indicates the information of the list of allowed manufacturers.

【Command Mode】 Privileged mode.

【Default Level】1

【Usage Guide】-

【Configuration Example]】1: Display the information of the allowed SSID list entries of WIDS.

```
AC-FS# show wids permitted ssid
```

【Prompt Information】-

【Platform Description】-

2.77 show wids rogue-ap detected

Displays the detection information of illegal APs that communicate with each other.

show wids rogue-ap detected

【Parameter Description】–

【Command Mode】 Privileged mode.

【Default Level】1

【Usage Guide】-

【Configuration Example】1: Display the detection information of illegal APs that communicate with each other.

```
AC-FS# show wids rogue-ap detected
```

【Prompt Information】-

【Platform Description】-

2.78 show wids statistics

Displays IDS attack detection information of WIDS.

show wids statistics

【Parameter Description】–

【Command Mode】 Privileged mode.

【Default Level】1

【Usage Guide】-

【Configuration Example]】1: Display the IDS attack detection information of WIDS.

```
AC-FS# show wids statistics
```

【Prompt Information】-

【Platform Description】-

2.79 show wids unknown-sta

Displays information about unknown STA list entries.

show wids unknown-sta

【Parameter Description】–

【Command Mode】 Privileged mode.

【Default Level】1

【Usage Guide】-

【Configuration Example]】1: Display the WIDS unknown name STA list entry information.

```
AC-FS# show wids unknown-sta
```

【Prompt Information】-

【Platform Description】-

2.80 show wids user-isolation permit-mac

Displays user quarantine allow list entry information for WIDS.

show wids user-isolation permit-mac

【Parameter Description】

【Command Mode】 Privileged mode.

【Default Level】1

【Usage Guide】-

【Configuration Example]】1: Display WIDS user isolation allow list entry information.

```
AC-FS# show wids user-isolation permit-mac
```

【Prompt Information】-

【Platform Description】-

2.81 show wids whitelist

Displays the whitelist entry information of WIDS.

show wids whitelist

【Parameter Description】–

【Command Mode】 Privileged mode.

【Default Level】1

【Usage Guide】-

【Configuration Example]】1: Display the whitelist entry information of WIDS.

```
AC-FS# show wids whitelist
```

【Prompt Information】-

【Platform Description】-

2.82 ssid-filter max

Configure the length of the ssid list for black and white lists based on ssid.

ssid-filter max num

Restore the ssid list length of black and white lists based on ssid to the default value.

no ssid-filter max

【Parameter Description】

Parameter	Description
num	Length of ssid list of black and white lists based on ssid, range (1~128).

【Default Configuration】 The default ssid list length is 64.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Set the length of the ssid list of black and white lists based on ssid to 40.

```
AC-FS(config-wids)# ssid-filter max 40
```

2: Restore the ssid list length of black and white lists based on ssid to the default value.

```
AC-FS(config-wids)#no ssid-filter max
```

【Verification】View through the show running-config command

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.83 ssid-filter blacklist mac-address in-ssid

Configure the blacklist entry for the specified SSID.

ssid-filter blacklist mac-address H.H.H[name another-name] in-ssid string

Deletes the blacklist entry of the specified MAC address of the specified SSID.

no ssid-filter blacklist mac-address H.H.H in-ssid string

【Parameter Description】

Parameter	Description
H.H.H	Indicates the MAC address of the ssid-based blacklist entry list.
string	Indicates the ssid value.
another-name	Indicates the alias of the MAC address in the specified SSID blacklist.

【Default Configuration】 The default is empty.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 If the information already exists in the SSID-based whitelist, the configuration is not allowed.

One another-name can correspond to multiple MAC addresses, but one MAC address can only correspond to one another-name. When another-name is not configured, another-name is empty.

【Configuration Example]】1: Set the device whose MAC address is 0000.0000.0001 as the blacklist of SSID: my-wlan.

```
AC-FS(config-wids)# ssid-filter blacklist mac-address 0000.0000.0001 in-ssid my-wlan
```

2: Delete the blacklist entry with MAC address 0000.0000.0001 from SSID: my-wlan.

```
AC-FS(config-wids)# no ssid-filter blacklist mac-address 0000.0000.0001 in-ssid my-wlan
```

【Verification】View through the show wids ssid-filter command.

【Prompt Information】1: If the configuration information already exists in the SSID-based whitelist, there will be an error message.

The mac[H.H.H] was filtered by white-list of SSID[string].

【Common Mistake】-

【Platform Description】-

2.84 ssid-filter blacklist max

Configure SSID-based blacklist column length.

ssid-filter blacklist max num

Restored SSID-based blacklist length to default.

no ssid-filter blacklist max

【Parameter Description】

Parameter	Description
num	Length of blacklist list based on SSID, range (1~256).

【Default Configuration】 The default SSID-based blacklist length is 256.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: The configuration is based on the blacklist length of 50.

```
AC-FS(config-wids)#ssid-filter blacklist max 50
```

2: Restore the SSID-based blacklist length to the default value.

```
AC-FS(config-wids)#no sid-filter blacklist max
```

【Verification】View through the show running-config command.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.85 ssid-filter whitelist mac-address in-ssid

Configure the whitelist entry for the specified SSID.

ssid-filter whitelist mac-address H.H.H[name another-name] in-ssid string

Deletes the whitelist entry of the specified MAC address of the specified SSID.

no ssid-filter whitelist mac-address H.H.H in-ssid string

【Parameter Description】

Parameter	Description
H.H.H	Indicates the MAC address of the whitelist entry list based on ssid.
string	Indicates the ssid value.
another-name	Indicates the alias of the MAC address in the specified SSID whitelist.

【Default Configuration】 The default is empty.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 If the information already exists in the SSID-based blacklist, the configuration is not allowed.

One another-name can correspond to multiple MAC addresses, but one MAC address can only correspond to one another-name. When another-name is not configured, another-name is empty.

【Configuration Example]】1: Set the device whose MAC address is 0000.0000.0001 as the whitelist of SSID: my-wlan.

```
AC-FS(config-wids)# ssid-filter whitelist mac-address 0000.0000.0001 in-ssid my-wlan
```

2: Delete the whitelist entry with MAC address 0000.0000.0001 from SSID: my-wlan.

```
AC-FS(config-wids)# no ssid-filter whitelist mac-address 0000.0000.0001 in-ssid my-wlan
```

【Verification】show wids ssid-filter command to view

【Prompt Information】1: If the entry already exists in the SSID-based blacklist, an error message will appear.

The mac[H.H.H] was filtered by black-list of SSID[string].

【Common Mistake】-

【Platform Description】-

2.86 ssid-filter whitelist max

Configure SSID-based whitelist length.

ssid-filter whitelist max num

Restored SSID-based whitelist length to default.

no ssid-filter whitelist max

【Parameter Description】

Parameter	Description
num	SSID-based whitelist length limit, range (1~256).

【Default Configuration】 The default SSID-based whitelist length is 256.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: The configuration is based on a whitelist with a list length of 50.

```
AC-FS(config-wids)#ssid-filter whitelist max 50
```

2: Restore the SSID-based whitelist length to the default value.

```
AC-FS(config-wids)#no sid-filter whitelist max
```

【Verification】View through the show running-config command

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.87 static-blacklist mac-address

Configure static blacklist entries.

static-blacklist mac-address H.H.H [name another-name]

Deletes the static blacklist entry of the specified MAC address.

no static-blacklist mac-address H.H.H

【Parameter Description】

Parameter	Description
H.H.H	Indicates the static blacklist entry list MAC address.
another-name	Indicates the alias of the MAC address in the static blacklist.

【Default Configuration】 The default is empty.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 If the configuration information already exists in the whitelist, the configuration is not allowed.

One another-name can correspond to multiple MAC addresses, but one MAC address can only correspond to one another-name. When another-name is not configured, another-name is empty.

【Configuration Example]】1: Set the device whose MAC address is 0000.0000.0001 as a static blacklist.

```
AC-FS(config-wids)# static-blacklist mac-address 0000.0000.0001
```

2: Delete the static blacklist entry with the MAC address of 0000.0000.0001.

```
AC-FS(config-wids)# no static-blacklist mac-address 0000.0000.0001
```

【Verification】-

【Prompt Information】1: The static blacklist configuration information is already in the whitelist, and an error message will appear.

```
The mac address has existed on the white list!
```

【Common Mistake】-

【Platform Description】-

2.88 static-blacklist max

Configure the length of the static blacklist.

static-blacklist max num

Restore allowed static blacklist length to default value.

no static-blacklist max

【Parameter Description】

Parameter	Description
num	Length of static blacklist list, range (1~2048).

【Default Configuration】 The default static blacklist length is 1024.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Set the length of the static blacklist to 1000.

```
AC-FS(config-wids)# static-blacklist max 1000
```

2: Restore the length of the static blacklist to the default value.

```
AC-FS(config-wids)#no static-blacklist max
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.89 user-isolation enable

Configuring and enabling Layer 2 user isolation on an AP or AC

user-isolation { ac | ap | ssid-ac | ssid-ap | wlan-id num } enable

Configure to disable the Layer 2 user isolation function on the AP or AC.

no user-isolation { ac | ap | ssid-ac | ssid-ap | wlan-id num } enable

【Parameter Description】

Parameter	Description
ac	Indicates that the AC-based Layer 2 user isolation function is enabled.
ssid-ac	Indicates that Layer 2 user isolation based on ac-ssid is enabled.
ap	Indicates that the AP-based Layer 2 user isolation function is enabled.
ssid-ap	Indicates that the Layer 2 user isolation function based on ap-ssid is enabled.
wlan-id num	Indicates that the Layer 2 user isolation function for interworking with the specified wlan-id (ssid) is enabled.

【Default Configuration】 It is closed by default.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Enable the AC-based Layer 2 user isolation function.

```
AC-FS(config-wids)# user-isolation ac enable
```

2: Disable the AC-based Layer 2 user isolation function.

```
AC-FS(config-wids)#no user-isolation ac enable
```

【Verification】View through the show ruuning-config command

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.90 user-isolation permit-mac

Configure the list of quarantine allowed MAC list entries.

user-isolation permit-mac H.H.H

Delete the list of quarantine allowed MAC list entries.

no user-isolation permit-mac H.H.H

【Parameter Description】

Parameter	Description
H.H.H	Indicates the MAC address of the Quarantine Allowed MAC List.

【Default Configuration】 The default is empty.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Set the MAC address of 0000.0000.0001 to allow the list of entries in the quarantine allowed MAC list.

```
AC-FS(config-wids)# user-isolation permit-mac 0000.0000.0001
```

2: Delete the list of allowed MAC list entries with the MAC address of 0000.0000.0001.

```
AC-FS(config-wids)#no user-isolation permit-mac 0000.0000.0001
```

【Verification】View through the show wids user-isolation permit-mac command.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.91 user-isolation permit-mac max

Configure the quarantine allowed MAC list length.

user-isolation permit-mac max num

Restore quarantine allowed MAC list length to default.

no user-isolation permit-mac max

【Parameter Description】

Parameter	Description
num	Isolation allowed MAC list length, range (1~2048).

【Default Configuration】 The default isolation allowed MAC list length is 1024.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Set the length of the isolation allowed MAC list to 1000.

```
AC-FS(config-wids)# user-isolation permit-mac max 1000
```

2: Restore the isolation allowed MAC list length to the default value.

```
AC-FS(config-wids)#no user-isolation permit-mac max
```

【Verification】View through the show ruuning-config command.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.92 whitelist mac-address

Configure whitelist entries.

whitelist mac-address H.H.H[name another-name]

Delete the whitelist entry of the specified MAC address.

no whitelist mac-address H.H.H

【Parameter Description】

Parameter	Description
H.H.H	Indicates the MAC address of the whitelist entry list.
another-name	Indicates the alias of the MAC address in the whitelist.

【Default Configuration】 The default is empty.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】 One another-name can correspond to multiple MAC addresses, but one MAC address can only correspond to one another-name. When another-name is not configured, another-name is empty.

【Configuration Example]】1: Set the device whose MAC address is 0000.0000.0001 as a whitelist.

```
AC-FS(config-wids)# whitelist mac-address 0000.0000.0001
```

2: Delete the whitelist entry with the MAC address of 0000.0000.0001.

```
AC-FS(config-wids)# no whitelistmac-address 0000.0000.0001
```

【Verification】View through the show wids whitelist command.

【Prompt Information】 1: If the whitelist configuration information is already in the static blacklist, there will be an error message.

The mac address has existed on black list.

【Common Mistake】-

【Platform Description】-

2.93 whitelist max

Configure the length of the whitelist list.

whitelist max num

Restore the whitelist list length.

no whitelist max

【Parameter Description】

Parameter	Description
num	Whitelist list length, range (1~2048).

【Default Configuration】 The default whitelist length is 1024.

【Command Mode】 WIDS configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Set the length of the whitelist list to 1000.

```
AC-FS(config-wids)# whitelist max 1000
```

2: Restore the length of the whitelist to the default value.

```
AC-FS(config-wids)#no whitelist max
```

【Verification】View through the show running-config command

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.94 wids

Configuration Enters WIDS configuration mode.

wids

【Parameter Description】–

【Default Configuration】 There is no Default Configuration.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】 This command is used to enter the WIDS configuration mode.

【Configuration Example】1: Enter wids configuration mode.

```
AC-FS(config)#wids
AC-FS(config-wids)#
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

3 CPP

3.1 cpu-protect type pps

Configure the bandwidth for the CPU port to receive packets of the specified type.

cpu-protect type { arp | bpdu | capwap-disc | d1x | dhcp-option82 | dhcp-relay-client | dhcp-relay-server | dhcps | igmp | ipmc | ipv6-nans | isis | lldp | ospf | ospfv3 | pim | pppoe | rip | ripng | tcp80 | tcp443 | vrrp } pps value

Restores the bandwidth of the CPU port for receiving packets of the specified type to the default value.

no cpu-protect type { arp | bpdu | capwap-disc | d1x | dhcp-option82 | dhcp-relay-client | dhcp-relay-server | dhcps | igmp | ipv6-nans | isis | lldp | ospf | ospfv3 | pim | pppoe | rip | ripng | tcp80 | tcp443 | vrrp } pps

【Parameter Description】

Parameter	Description
arp	ARP protocol packet type.
bpdu	IEEE BPDU protocol message type.
capwap-disc	CAPWAP DISCOVER protocol message type.
d1x	802.1x EAPOL message types.
dhcp-option82	DHCP OPTION82 message type.
dhcp-relay-client	DHCP RELAY CLIENT message type.
dhcp-relay-server	DHCP RELAY SERVER message type.
dhcps	DHCP SNOOPING packet type.
igmp	IGMP protocol message type.
ipmc	IPv4 multicast datagram type.
ipv6-nans	IPv6 Neighbor Discovery Protocol Packet Type.
isis	ISIS protocol message type.
lldp	LLDP protocol packet type.
ospf	OSPF protocol packet type.
ospfv3	OSPF verion3 protocol packet type.
pim	PIM protocol message type.
pppoe	PPPOE protocol packet type.
rip	IPv4 RIP protocol packet type.
ripng	IPv6 RIP protocol packet type.
tcp80	Web Authentication Redirect Packet Type.
tcp443	HTTPS packet type.
vrrp	VRRP protocol packet type.
value	The upper limit of the number of packets per second, the configurable range is 0~148810pps.

【Default Configuration】 Provide different default values according to different products.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command is used to configure the bandwidth of the CPU port to receive the specified type of packets.

【Configuration Example]】1: Configure the bandwidth of the CPU port to receive arp packets to 200pps.

```
AC-FS(config)# cpu-protect type arp pps 200
```

【Verification】1: Use the show cpu-protect summary command to check whether the configuration is correct

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

3.2 mgmt-ratelimit

Configure the rate limit function for wireless management packets.

mgmt-ratelimit { disable | per-cti pps value | total pps value }

Restore the wireless management packet rate limit function configuration to the default value.

no mgmt-ratelimit { disable | per-cti pps | total pps }

【Parameter Description】

Parameter	Description
disable	Disable the wireless management packet rate limit function.
per-cti pps value	CTI-based wireless management packet rate limit threshold.
total pps value	AC-based wireless management packet rate limit threshold.

【Default Configuration】 By default, the CPU port's rate-limiting function for receiving wireless management packets is enabled, and this function is only supported on AC devices; CTI-based default wireless management packet bandwidth threshold: 8pps;

The default wireless management packet bandwidth threshold based on the AC machine: different default values are provided

according to different AC products.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command is used to configure the bandwidth control function and threshold for the CPU port to receive wireless management packets.

【Configuration Example]】1: Configure the bandwidth of the AC-based CPU port to receive wireless management packets to 200pps.

```
AC-FS(config)#mgmt-ratelimit total pps 200
```

【Verification】1: Use the show running-config command to check whether the configuration is correct

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

3.3show cpu-protect summary

Displays the bandwidth configuration for receiving various types of packets on the CPU port

show cpu-protect summary

【Parameter Description】–

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】 This command is used to display and configure the bandwidth of the CPU port to receive various types of packets.

【Configuration Example]】1: Display the bandwidth configuration of the CPU port receiving various types of packets.

```
AC-FS# show cpu-protect summary
```

【Prompt Information】-

【Platform Description】-

3.4 show cpu-protect type

Displays statistics on packets of the specified type.

show cpu-protect type { arp | bpdu | capwap-disc | d1x | dhcp-option82 | dhcp-relay-client | dhcp-relay-server | dhcps | igmp | ipmc | ipv6-nans | isis | lldp | ospf | ospfv3 | pim | pppoe | rip | ripng | tcp80 | vrrp }

【Parameter Description】

Parameter	Description
arp	ARP protocol packet type
bpdu	IEEE BPDU protocol message type
capwap-disc	CAPWAP DISCOVER protocol message type
d1x	802.1x EAPOL message types
dhcp-option82	DHCP OPTION82 message type
dhcp-relay-client	DHCP RELAY CLIENT message type
dhcp-relay-server	DHCP RELAY SERVER message type
dhcps	DHCP SNOOPING packet type
igmp	IGMP protocol message type
ipmc	IPv4 multicast datagram type
ipv6-nans	IPv6 Neighbor Discovery Protocol Packet Type
isis	ISIS protocol message type
lldp	LLDP protocol packet type
ospf	OSPF protocol packet type
ospfv3	OSPF version3 packet type
pim	PIM protocol message type
pppoe	PPPOE protocol packet type
rip	IPv4 RIP packet type
ripng	IPv6 RIP packet type
tcp80	Web Authentication Redirect Packet Type
vrrp	VRRP protocol packet type

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】 This command displays the statistics of packets of the specified type.

【Configuration Example]】1: Display the type statistics of arp packets.

```
AC-FS#show cpu-protect type arp
```

【Prompt Information】-

【Platform Description】-

3.5show mgmt-ratelimit cti

Display the packet statistics of the wireless management packets of the specified CTI.

show mgmt-ratelimit cti ifx

【Parameter Description】

Parameter	Description
cti ifx	Specifies the interface index value of the CTI.

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】 This command is used to display the packet statistics of the wireless management packets of the specified CTI

【Configuration Example]】1: Display the wireless management packet statistics of the CTI with the interface index value of 9.

```
AC-FS#show mgmt-ratelimit cti 9
```

【Prompt Information】-

【Platform Description】-

3.6show mgmt-ratelimit summary

Display the packet statistics of the wireless management packets of the AC

show mgmt-ratelimit summary

【Parameter Description】–

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】 This command is used to display the statistics of wireless management packets based on the AC.

【Configuration Example]】1: Display the wireless management packet statistics of the AC.

```
AC-FS#show mgmt-ratelimit summary
```

【Prompt Information】-

【Platform Description】-

4 NFPP

4.1arp-guard attack-threshold

Configure a global attack waterline, that is, when the packet speed exceeds the attack waterline, an attack is considered to exist.

arp-guard attack-threshold { per-src-ip | per-src-mac | per-port } pps

Delete the attack waterline configuration and restore it to the Default Configuration.

no arp-guard attack-threshold { per-src-ip | per-src-mac | per-port }

Restore Default Configuration.

default arp-guard attack-threshold { per-src-ip | per-src-mac | per-port }

【Parameter Description】

Parameter	Description
per-src-ip	Configure the attack waterline for each source IP address.
per-src-mac	Configure the attack watermark for each source MAC address.
per-port	Configure the attack waterline for each port.
pps	Attack waterline, the unit is the number of packets per second, and the value range is [1,9999].

【Default Configuration】 The default attack watermark is 16 per second per source IP address and per source MAC address, and 200 per second per port.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】 The attack waterline cannot be less than the speed limit waterline.

【Configuration Example]】 1: Configure the ARP anti-attack global attack waterline, the source IP-based attack waterline is 2pps, the source MAC attack waterline is 3pps, and the source port-based attack waterline is 50pps.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# arp-guard attack-threshold per-src-ip 2
AC-FS(config-nfpp)# arp-guard attack-threshold per-src-mac 3
AC-FS(config-nfpp)# arp-guard attack-threshold per-port 50
```

【**Verification**】Use show nfpp arp-guard summary to view configuration information

【**Prompt Information**】-

【**Common Mistake**】-

【**Platform Description**】-

4.2arp-guard enable

This command is used to globally enable ARP anti-attack function.

arp-guard enable

Disable ARP anti-attack function

no arp-guard enable

Restore Default Configuration

default arp-guard enable

【**Parameter Description**】–

【**Default Configuration**】 The default ARP anti-attack function is enabled

【**Command Mode**】 NFPP configuration mode

【**Default Level**】 14

【**Usage Guide**】-

【**Configuration Example]**】1: Configure to enable ARP anti-attack function globally

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# arp-guard enable
```

【Verification】Use show nfpp arp-guard summary to view configuration information

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.3arp-guard isolate-period

This command is used to configure the global isolation time

arp-guard isolate-period { seconds | permanent }

Delete the quarantine time configuration and restore to Default Configuration

no arp-guard isolate-period

Restore Default Configuration

default arp-guard isolate-period

【Parameter Description】

Parameter	Description
seconds	The isolation time, in seconds, in the range of 0 or [30, 86400].
permanent	permanent isolation

【Default Configuration】 The default value of the global isolation time is 0, that is, no isolation.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the ARP anti-attack global isolation time to 180 seconds.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# arp-guard isolate-period 180
```

【Verification】Use show nfpp arp-guard summary to view configuration information

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.4arp-guard monitored-host-limit

This command is used to configure the maximum number of monitored hosts supported.

arp-guard monitored-host-limit number

Delete the maximum number of monitored hosts configuration and restore to Default Configuration

no arp-guard monitored-host-limit

Restore Default Configuration

default arp-guard monitored-host-limit

【Parameter Description】

Parameter	Description
number	The maximum number of monitored hosts supported, ranging from 1 to 4294967295.

【Default Configuration】 The maximum number of monitored hosts is 1000 by default.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】If the number of monitored hosts has reached the default 1000, and the administrator sets the maximum number of

monitored hosts to less than 1000, the existing monitored hosts will not be deleted, but the message "%ERROR: The value that you configured is smaller than current monitored hosts 1000 (the number of monitored hosts configured), please clear a part of monitored hosts." to remind the administrator that the configuration does not take effect, and some hosts that have been monitored need to be deleted.

When the monitored host table is full, print the log "% NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 (configured monitored hosts) monitored hosts." to remind the administrator.

【Configuration Example]】 1: Configure the maximum number of monitored hosts for ARP anti-attack to 200.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# arp-guard monitored-host-limit 200
```

【Verification】 Use show nfpp arp-guard summary to view configuration information.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

4.5arp-guard monitor-period

This command is used to configure monitoring time.

arp-guard monitor-period seconds

Delete the monitoring time configuration and restore it to the Default Configuration

no arp-guard monitor-period

Restore Default Configuration

default arp-guard monitor-period

【Parameter Description】

Parameter	Description
seconds	Monitoring time, the unit is second, the value range is [180, 86400].

【Default Configuration】 The default value of monitoring time is 600 seconds.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】When an attacker is detected, if the isolation time is 0, the software will monitor the attacker, and the timeout is the monitoring time. During the software monitoring process, when the isolation time is configured as a non-zero value, the attackers monitored by the software will be automatically isolated, and the timeout is set as the isolation time. The monitoring time is only meaningful when the isolation time is 0.

If the isolation time is changed from a non-zero value to zero, the attacker of the relevant port will be deleted directly instead of software monitoring.

【Configuration Example]】1: Configure the ARP anti-attack monitoring time to 180 seconds.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# arp-guard monitor-period 180
```

【Verification】Use show nfpp arp-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.6arp-guard rate-limit

Configure global speed limit waterline

arp-guard rate-limit { per-src-ip | per-src-mac | per-port } pps

Delete the speed limit waterline configuration and restore to Default Configuration

no arp-guard rate-limit { per-src-ip | per-src-mac | per-port }

Restore Default Configuration

default arp-guard rate-limit { per-src-ip | per-src-mac | per-port }

【Parameter Description】

Parameter	Description
per-src-ip	Rate limiting per source IP address.
per-src-mac	Rate limiting per source MAC address.
per-port	Speed limit on each port.
pps	The speed limit waterline value, the value range is [1,9999].

【Default Configuration】 The default rate limit watermark per source IP address and each source MAC address is 8 per second, and the default rate limit watermark per port is 100 per second.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the ARP anti-attack full speed limit waterline, based on the source IP speed limit waterline 2pps, based on the source MAC speed limit waterline 3pps, based on the source port speed limit waterline 50pps.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# arp-guard rate-limit per-src-ip 2
AC-FS(config-nfpp)# arp-guard rate-limit per-src-mac 3
AC-FS(config-nfpp)# arp-guard rate-limit per-port 50
```

【Verification】Use show nfpp arp-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.7arp-guard scan-threshold

Configure the global scan watermark.

arp-guard scan-threshold pkt-cnt

Delete the scan waterline configuration and restore to the Default Configuration

no arp-guard scan-threshold

Restore Default Configuration

default arp-guard scan-threshold

【Parameter Description】

Parameter	Description
pkt-cnt	Sweep waterline value, the value range is [1,9999].

【Default Configuration】 The default scan watermark is 15, and the time unit is 10 seconds.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】 If more than 15 ARP packets are received in 10 seconds, the link layer source MAC address is fixed but the source IP address changes, or the link layer source MAC address is changed.

The address and the source IP address are fixed and the destination IP address is constantly changing, it is considered to be suspected of scanning.

【Configuration Example]】1: Configure the ARP anti-attack full scan waterline to 20pps.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# arp-guard scan-threshold 20
```

【Verification】Use show nfpp arp-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.8arp-guard trusted-host

If the administrator wants to not monitor a host, that is, to trust the host, it can be configured through this command.

arp-guard trusted-host ip mac

Delete unmonitored trusted hosts

no arp-guard trusted-host { all | ip mac }

Clear Do not monitor trusted hosts

default arp-guard trusted-host

【Parameter Description】

Parameter	Description
ip	IP address.
mac	MAC address.
all	Used with no to remove all trusted hosts configuration.

【Default Configuration】-

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】 If the administrator wants to not monitor a certain host, that is, express trust in the host, it can be configured through this command. The ARP packets sent by the trusted host to the CPU will be allowed to be sent to the CPU without any rate limit and alarm processing.

A maximum of 500 trusted hosts can be set.

【Configuration Example]】1: Configure the host with IP 1.1.1.1 and MAC 0000.0000.1111 as a trusted host for ARP anti-attack.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)#arp-guard trusted-host 1.1.1.0 0000.0000.1111
```

【Verification】Use show nfpp arp-guard trusted-host to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.9 clear nfpp arp-guard hosts

Clear the monitored host, if the host is quarantined, it needs to be released

clear nfpp arp-guard hosts [vlan vid] [interface interface-id] [ip-address | mac-address]

【Parameter Description】

Parameter	Description
vid	virtual LAN number.
interface-id	port name.
ip-address	IP address.
mac-address	MAC address.

【Default Configuration】 Privileged Mode

【Command Mode】 If there is no parameter, it means to clear all monitored hosts.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: De-isolate the ARP anti-attack host on port g 0/1 of VLAN 1.

```
AC-FS# clear nfpp arp-guard hosts vlan 1 interface g0/1
```

【Verification】Use show nfpp arp-guard hosts to view user information

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.10 clear nfpp arp-guard scan

Clear the ARP scan table.

clear nfpp arp-guard scan

【Parameter Description】–

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Clear the ARP anti-attack scan table.

```
AC-FS# clear nfpp arp-guard scan
```

【Verification】Use show nfpp arp-guard scan to view scan table information

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.11 clear nfpp dhcp-guard hosts

Clearing a user means releasing the user from quarantine.

clear nfpp dhcp-guard hosts [vlan vid] [interface interface-id] [mac-address]

【Parameter Description】

Parameter	Description
vid	virtual LAN number.
interface-id	port name.
mac-address	MAC address.

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 If there is no Parameter, it means to clear all the isolated users.

【Configuration Example]】1: Release the DHCP anti-attack users on port g 0/1 of VLAN 1 from isolation.

```
AC-FS# clear nfpp dhcp-guard hosts vlan 1 interface g0/1
```

【Verification】Use show nfpp dhcp-guard hosts to view user information

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.12 clear nfpp dhcpv6-guard hosts

Clear the user, i.e. release the user from quarantine

clear nfpp dhcpv6-guard hosts [vlan vid] [interface interface-id] [mac-address]

【Parameter Description】

Parameter	Description
vid	Virtual LAN number.
interface-id	port name.
mac-address	MAC address.

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 If there is no Parameter, it means to clear all the isolated users.

【Configuration Example]】1: Release the DHCPv6 anti-attack users on port g 0/1 of VLAN 1 from isolation.

```
AC-FS# clear nfpp dhcpv6-guard hosts vlan 1 interface g0/1
```

【Verification】Use show nfpp dhcpv6-guard hosts to view user information

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.13 clear nfpp icmp-guard hosts

Clear the monitored host, if the host is quarantined, it needs to be released.

clear nfpp icmp-guard hosts [vlan vid] [interface interface-id] [ip-address]

【Parameter Description】

Parameter	Description
vid	virtual LAN number.
interface-id	port name.
ip-address	IP address.

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 If there is no parameter, it means to clear all monitored hosts.

【Configuration Example]】1: Clear the ICMP anti-attack monitored host of VLAN 1 port g 0/1.

```
AC-FS# clear nfpp icmp-guard hosts vlan 1 interface g 0/1
```

【Verification】Use show nfpp icmp-guard hosts to view user information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.14 clear nfpp ip-guard hosts

Clear the monitored host, if the host is quarantined, it needs to be released.

clear nfpp ip-guard hosts [vlan vid] [interface interface-id] [ip-address]

【Parameter Description】

Parameter	Description
vid	virtual LAN number.
interface-id	port name.
ip-address	IP address.

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 If there is no parameter, it means to clear all monitored hosts.

【Configuration Example]】1: De-isolate the IP anti-attack host of port g 0/1 of VLAN 1.

```
AC-FS# clear nfpp ip-guard hosts vlan 1 interface g0/1
```

【Verification】Use show nfpp ip-guard hosts to view user information

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.15 clear nfpp log

Flush the NFPP log buffer

clear nfpp log

【Parameter Description】–

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Clear the log buffer of NFPP.

```
AC-FS# clear nfpp log
32 log-buffer entries were cleared.
```

【Verification】Use show nfpp log to view log information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.16cpu-protect sub-interface percent

This command is used to configure the percentage of each type of packets occupying the queue.

cpu-protect sub-interface { manage | protocol | route } percent percent_vaule

Delete the configuration of the percentage of queues occupied by each type of packets and restore to the Default Configuration.

no cpu-protect sub-interface { manage | protocol | route } percent

Restore Default Configuration.

default cpu-protect sub-interface { manage | protocol | route } percent

【Parameter Description】

Parameter	Description

manage	Designated management class.
protocol	Specify the protocol class.
route	Specify forwarding class.
percent_vaule	percentage, from 1 to 100.

【Default Configuration】 The percentage of the buffer occupied by the management class (Manage) is 30

The forwarding class (Route) occupies a buffer percentage of 25

Protocol class (Protocol) occupies a buffer percentage of 45

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: The percentage of the buffer occupied by configuration management packets is 60

AC-FS(config)# cpu-protect sub-interface manage percent 60

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.17 cpu-protect sub-interface pps

This command is used to configure the traffic bandwidth of each type of packet.

cpu-protect sub-interface { manage | protocol | route } pps pps_vaule

Delete the traffic bandwidth configuration for each type of packet and restore it to the Default Configuration

no cpu-protect sub-interface { manage | protocol | route } pps

Restore Default Configuration

default cpu-protect sub-interface { manage | protocol | route } pps

【Parameter Description】

Parameter	Description
manage	Designated management class.
protocol	Specify the protocol class.
route	Specify forwarding class.
pps_vaule	Speed limit waterline, the value range is 1-100000.

【Default Configuration】 See product feature document

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the management packet traffic bandwidth to 2000pps.

```
AC-FS(config)# cpu-protect sub-interface manage pps 2000
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.18dhcp-guard attack-threshold

Configure a global attack waterline, that is, when the packet speed exceeds the attack waterline, an attack is considered to exist.

dhcp-guard attack-threshold { per-src-mac | per-port } pps

Delete the attack waterline configuration and restore to Default Configuration.

no dhcp-guard attack-threshold { per-src-mac | per-port }

Restore Default Configuration.

default dhcp-guard attack-threshold { per-src-mac | per-port }

【Parameter Description】

Parameter	Description
per-src-mac	Configure the attack watermark for each source MAC address.
per-port	Configure the attack waterline for each port.
pps	Attack waterline, the unit is the number of packets per second, and the value range is [1,9999].

【Default Configuration】 The default attack threshold of each source MAC address is 10 per second, and the default attack threshold of each port is 300 per second.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure DHCP anti-attack global attack waterline, based on the source MAC attack waterline 15pps, based on the source port attack waterline 200pps.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# dhcp-guard attack-threshold per-src-mac 15
AC-FS(config-nfpp)# dhcp-guard attack-threshold per-port 200
```

【Verification】Use show nfpp dhcp-guard summary to view configuration information

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.19dhcp-guard enable

This command is used to enable the DHCP attack defense function.

dhcp-guard enable

Disable DHCP anti-attack function.

no dhcp-guard enable

Restore Default Configuration.

default dhcp-guard enable

【Parameter Description】–

【Default Configuration】 The port is not configured with the DHCP anti-attack switch, and the global switch is used.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Configure to enable DHCP anti-attack function globally.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# dhcp-guard enable
```

【Verification】Use show nfpp dhcp-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.20dhcp-guard isolate-period

This command is used to configure the global isolation time.

dhcp-guard isolate-period { seconds | permanent }

Delete the quarantine time configuration and restore to Default Configuration.

no dhcp-guard isolate-period

Restore Default Configuration.

default dhcp-guard isolate-period

【Parameter Description】

Parameter	Description
seconds	Isolation time, the unit is seconds, the value range is 0 or [30, 86400], 0 means no isolation.
permanent	permanent isolation.

【Default Configuration】 The default value of the global isolation time is 0, that is, no isolation.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】The isolation time for attackers is divided into global isolation time and port-based isolation time (ie, local isolation time). For a port, if the port-based isolation time is not configured, the global isolation time is used; otherwise, the port-based isolation time is used.

【Configuration Example]】1: Configure the DHCP anti-attack global isolation time to 180 seconds.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# dhcp-guard isolate timeout 180
```

【Verification】Use show nfpp dhcp-guard summary to view configuration information

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.21dhcp-guard monitored-host-limit

This command is used to configure the maximum number of monitored hosts supported.

dhcp-guard monitored-host-limit number

Delete the maximum number of monitored hosts configuration and restore to Default Configuration.

no dhcp-guard monitored-host-limit

Restore Default Configuration.

default dhcp-guard monitored-host-limit

【Parameter Description】

Parameter	Description
number	The maximum number of monitored hosts supported, in the range 1 to 4294967295.

【Default Configuration】 The maximum number of monitored hosts is 1000 by default

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】 If the number of monitored hosts has reached the default 1000, and the administrator sets the maximum number of monitored hosts to less than 1000, the existing monitored hosts will not be deleted, but the message "%ERROR: The value that you configured is smaller than current monitored hosts 1000 (the number of monitored hosts configured), please clear a part of monitored hosts." to remind the administrator that the configuration does not take effect, and some hosts that have been monitored need to be deleted.

When the monitored host table is full, print the log "% NFPP_DHCP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 (configured number of monitored hosts) monitored hosts." to remind the administrator.

【Configuration Example]】1: Configure the maximum number of monitored hosts for DHCP anti-attack to 200.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# dhcp-guard monitored-host-limit 200
```

【Verification】Use show nfpp dhcp-guard summary to view configuration information

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.22dhcp-guard monitor-period

This command is used to configure monitoring time.

dhcp-guard monitor- period seconds

Delete the monitoring time configuration and restore it to the Default Configuration.

no dhcp-guard monitor-period

Restore Default Configuration.

default dhcp-guard monitor-period

【Parameter Description】

Parameter	Description
seconds	Monitoring time, the unit is second, the value range is [180, 86400].

【Default Configuration】 The default value of the global monitoring time is 600 seconds.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】When an attacker is detected, if the isolation time is 0, the software will monitor the attacker, and the timeout is the monitoring time. During the software monitoring process, when the isolation time is configured as a non-zero value, the attackers monitored by the software will be automatically isolated, and the timeout is set as the isolation time. The monitoring time is only meaningful when the isolation time is 0.

If the isolation time is changed from a non-zero value to zero, the attacker of the relevant port will be deleted directly instead of software monitoring.

【Configuration Example]】1: Configure the DHCP anti-attack monitoring time to 180 seconds.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# dhcp-guard monitor-period 180
```

【Verification】Use show nfpp dhcp-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.23dhcp-guard rate-limit

Configure the global speed limit waterline.

dhcp-guard rate-limit { per-src-mac | per-port } pps

Delete the speed limit waterline configuration and restore to Default Configuration

no dhcp-guard rate-limit { per-src-mac | per-port }

Restore Default Configuration

default dhcp-guard rate-limit { per-src-mac | per-port }

【Parameter Description】

Parameter	Description
per-src-mac	Rate limiting per source MAC address.
per-port	Speed limit on each port.
pps	The speed limit waterline value, the value range is [1,9999].

【Default Configuration】 The default rate limit threshold for each source MAC address is 5 per second, and the default rate threshold for each port is 150 per second.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the DHCP anti-attack full speed limit waterline, based on the source MAC speed limit waterline 8pps, based on the source port speed limit waterline 100pps.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# dhcp-guard rate-limit per-src-mac 8
AC-FS(config-nfpp)# dhcp-guard rate-limit per-port 100
```

【Verification】Use show nfpp dhcp-guard summary to view configuration information

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.24dhcp-guard trusted-host

If the administrator wants to not monitor a host, that is, to trust the host, it can be configured through this command.

dhcp-guard trusted-host mac

Delete unmonitored trusted hosts

no dhcp-guard trusted-host { all | mac }

Clear Do not monitor trusted hosts

default dhcp-guard trusted-host

【Parameter Description】

Parameter	Description
mac	MAC address.
all	Used with no to remove all trusted hosts configuration.

【Default Configuration】-

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】 If the administrator wants to not monitor a certain host, that is, express trust in the host, it can be configured through this command. The DHCP packets sent by the trusted host to the CPU will be allowed to be sent to the CPU without any rate limit and alarm processing.

A maximum of 500 trusted hosts can be set.

【Configuration Example]】1: Configure the host whose MAC is 0000.0000.1111 as a trusted host for DHCP anti-attack.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)#dhcp-guard trusted-host 0000.0000.1111
```

【Verification】Use show nfpp dhcp-guard trusted-host to view configuration information

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.25dhcpv6-guard attack-threshold

Configure a global attack waterline, that is, when the packet speed exceeds the attack waterline, an attack is considered to exist.

dhcpv6-guard attack-threshold { per-src-mac | per-port } pps

Delete the attack waterline configuration and restore it to the Default Configuration.

no dhcpv6-guard attack-threshold { per-src-mac | per-port }

Restore Default Configuration.

default dhcpv6-guard attack-threshold { per-src-mac | per-port }

【Parameter Description】

Parameter	Description
per-src-mac	Configure the attack watermark for each source MAC address.
per-port	Configure the attack waterline for each port.
pps	Attack waterline, the unit is the number of packets per second, and the value range is [1,9999].

【Default Configuration】 The default attack threshold of each source MAC address is 10 per second, and the default attack threshold of each port is 300 per second.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the DHCPv6 anti-attack global attack waterline, which is 15pps based on the source MAC and 200pps based on the source port.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# dhcpv6-guard attack-threshold per-src-mac 15
AC-FS(config-nfpp)# dhcpv6-guard attack-threshold per-port 200
```

【Verification】Use show nfpp dhcpv6-guard summary to view configuration information

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.26dhcpv6-guard enable

This command is used to enable the DHCPv6 attack defense function.

dhcpv6-guard enable

Disable DHCPv6 anti-attack function.

no dhcpv6-guard enable

Restore Default Configuration.

default dhcpv6-guard enable

【Parameter Description】–

【Default Configuration】 The port is not configured with the DHCPv6 anti-attack switch, and the global switch is used.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Configure to enable DHCPv6 anti-attack function globally.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# dhcpv6-guard enable
```

【Verification】Use show nfpp dhcpv6-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.27dhcpv6-guard isolate-period

This command is used to configure the global isolation time.

dhcpv6-guard isolate-period { seconds | permanent }

Delete the quarantine time configuration and restore to Default Configuration.

no dhcpv6-guard isolate-period

Restore Default Configuration.

default dhcpv6-guard isolate-period

【Parameter Description】

Parameter	Description
seconds	Isolation time, the unit is seconds, the value range is 0 or [30, 86400], 0 means no isolation.
permanent	permanent isolation

【Default Configuration】 The default value of the global isolation time is 0, that is, no isolation.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】The isolation time for attackers is divided into global isolation time and port-based isolation time (ie, local isolation time). For a port, if the port-based isolation time is not configured, the global isolation time is used; otherwise, the port-based isolation time is used.

【Configuration Example]】1: Configure the DHCPv6 anti-attack global isolation time to 180 seconds.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# dhcpv6-guard isolate timeout 180
```

【Verification】Use show nfpp dhcpv6-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.28dhcpv6-guard monitored-host-limit

This command is used to configure the maximum number of monitored hosts supported.

dhcpv6-guard monitored-host-limit number

Delete the maximum number of monitored hosts configuration and restore to Default Configuration.

no dhcpv6-guard monitored-host-limit

Restore Default Configuration.

default dhcpv6-guard monitored-host-limit

【Parameter Description】

Parameter	Description
number	The maximum number of monitored hosts supported, in the range 1 to 4294967295.

【Default Configuration】 The maximum number of monitored hosts is 1000 by default.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】 If the number of monitored hosts has reached the default 1000, the administrator should set the maximum number of monitored hosts to be less than 1000.

The existing monitored hosts will be deleted, but the message "%ERROR: The value that you configured is smaller than current monitored hosts 1000 (the number of monitored hosts configured), please clear a part of monitored hosts." will be printed to remind the management The member configuration does not take effect, and some hosts that have been monitored need to be deleted.

When the monitored host table is full, print the log "% NFPP_DHCP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 (configured number of monitored hosts) monitored hosts." to remind the administrator.

【Configuration Example]】1: Configure the maximum number of monitored hosts for DHCPv6 anti-attack to 200.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# dhcp-guard monitored-host-limit 200
```

【Verification】Use show nfpp dhcpv6-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.29dhcpv6-guard monitor-period

This command is used to configure monitoring time.

dhcpv6-guard monitor- period seconds

Delete the monitoring time configuration and restore it to the Default Configuration.

no dhcpv6-guard monitor-period

Restore Default Configuration.

default dhcpv6-guard monitor-period

【Parameter Description】

Parameter	Description

seconds	Monitoring time, the unit is second, the value range is [180, 86400].

【Default Configuration】 The default value of the global monitoring time is 600 seconds.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】 When an attacker is detected, if the isolation time is 0, the software will monitor the attacker, and the timeout is the monitoring time. During the software monitoring process, when the isolation time is configured as a non-zero value, the attackers monitored by the software will be automatically isolated, and the timeout is set as the isolation time. The monitoring time is only meaningful when the isolation time is 0.

If the isolation time is changed from a non-zero value to zero, the attacker of the relevant port will be deleted directly instead of software monitoring.

【Configuration Example]】 1: Configure the DHCPv6 anti-attack monitoring time to 180 seconds.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# dhcpv6-guard monitor-period 180
```

【Verification】 Use show nfpp dhcpv6-guard summary to view configuration information.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

4.30dhcpv6-guard rate-limit

Configure global speed limit waterline.

dhcpv6-guard rate-limit { per-src-mac | per-port } pps

Delete the speed limit waterline configuration and restore to Default Configuration.

no dhcpv6-guard rate-limit { per-src-mac | per-port }

Restore Default Configuration.

default dhcpv6-guard rate-limit { per-src-mac | per-port }

【Parameter Description】

Parameter	Description
per-src-mac	Rate limiting per source MAC address.
per-port	Speed limit on each port.
pps	The speed limit waterline value, the value range is [1,9999].

【Default Configuration】 The default rate limit threshold for each source MAC address is 5 per second, and the default rate threshold for each port is 150 per second.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the DHCPv6 anti-attack full speed limit waterline, based on the source MAC speed limit waterline of 8pps, based on the source port speed limit waterline of 100pps.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# dhcpv6-guard rate-limit per-src-mac 8
```

AC-FS(config-nfpp)# dhcpv6-guard rate-limit per-port 100

【Verification】Use show nfpp dhcpv6-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.31dhcpv6-guard trusted-host

If the administrator wants to not monitor a host, that is, to trust the host, it can be configured through this command.

dhcpv6-guard trusted-host mac

Delete unmonitored trusted hosts

no dhcpv6-guard trusted-host { all | mac }

Clear Do not monitor trusted hosts

default dhcpv6-guard trusted-host

【Parameter Description】

Parameter	Description
mac	MAC address.
all	Used with no to remove all trusted hosts configuration.

【Default Configuration】-

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】 If the administrator wants to not monitor a certain host, that is, express trust in the host, it can be configured through this command. The DHCPv6 packets sent by the trusted host to the CPU will be allowed to be sent to the CPU without any rate limit and alarm processing.

A maximum of 500 trusted hosts can be set.

【Configuration Example]】1: Configure the host whose MAC is 0000.0000.1111 as a trusted host for DHCPv6 anti-attack.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)#dhcpv6-guard trusted-host 0000.0000.1111
```

【Verification】Use show nfpp dhcpv6-guard trusted-host to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.32 icmp-guard attack-threshold

Configure a global attack waterline, that is, when the packet speed exceeds the attack waterline, an attack is considered to exist.

icmp-guard attack-threshold { per-src-ip | per-port } pps

Delete the attack waterline configuration and restore it to the Default Configuration.

no icmp-guard attack-threshold { per-src-ip | per-port }

Restore Default Configuration.

default icmp-guard attack-threshold { per-src-ip | per-port }

【Parameter Description】

Parameter	Description
per-src-ip	Configure the attack waterline for each source IP address.
per-port	Configure the attack waterline for each port.
pps	Attack waterline, the unit is the number of packets per second, and the value range is [1,9999].

【Default Configuration】 See the product feature document.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example]】1: Configure the ICMP anti-attack global attack waterline, the attack waterline based on the source IP is 600pps, and the attack waterline based on the source port is 1200pps.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# icmp-guard attack-threshold per-src-ip 600
AC-FS(config-nfpp)# icmp-guard attack-threshold per-port 1200
```

【Verification】 Use show nfpp icmp-guard summary to view configuration information.

【Prompt Information】 -

【Common Mistake】-

【Platform Description】-

4.33icmp-guard enable

This command is used to enable the ICMP attack defense function.

icmp-guard enable

Disable ICMP anti-attack function

no icmp-guard enable

Restore Default Configuration

default icmp-guard enable

【Parameter Description】–

【Default Configuration】 The default ICMP attack defense function is enabled

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure to enable ICMP anti-attack function globally.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# icmp-guard enable
```

【Verification】Use show nfpp icmp-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.34icmp-guard isolate-period

This command is used to configure the global isolation time.

icmp-guard isolate-period { seconds | permanent }

Delete the quarantine time configuration and restore to Default Configuration.

no icmp-guard isolate-period

Restore Default Configuration.

default icmp-guard isolate-period

【Parameter Description】

Parameter	Description
seconds	Isolation time, the unit is seconds, the value range is 0 or [30, 86400], 0 means no isolation.
permanent	permanent isolation.

【Default Configuration】 The default value of the global isolation time is 0, that is, no isolation.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】The isolation time for attackers is divided into global isolation time and port-based isolation time (ie, local isolation time). For a port, if the port-based isolation time is not configured, the global isolation time is used; otherwise, the port-based isolation time is used.

【Configuration Example]】1: Configure the ICMP anti-attack global isolation time to 180 seconds.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# icmp-guard enable
```

【Verification】Use show nfpp icmp-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.35 icmp-guard monitored-host-limit

This command is used to configure the maximum number of monitored hosts supported.

icmp-guard monitored-host-limit number

Delete the maximum number of monitored hosts configuration and restore to Default Configuration.

no icmp-guard monitored-host-limit

Restore Default Configuration.

default icmp-guard monitored-host-limit

【Parameter Description】

Parameter	Description
number	The maximum number of monitored hosts supported, ranging from 1 to 4294967295.

【Default Configuration】 The maximum number of monitored hosts is 1000 by default.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】If the number of monitored hosts has reached the default 1000, and the administrator sets the maximum number of monitored hosts to less than 1000, the existing monitored hosts will not be deleted, but the message "%ERROR: The value that you configured is smaller than current monitored hosts 1000 (the number of monitored hosts configured), please clear a part of monitored hosts." to remind the administrator that the configuration does not take effect, and some hosts that have been monitored need to be deleted.

When the monitored hosts are full, print the log "% NFPP_ICMP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 (configured monitored hosts) monitored hosts." to remind the administrator.

【Configuration Example]】1: Configure the maximum number of monitored hosts for ICMP anti-attack to 200.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# icmp-guard monitored-host-limit 200
```

【Verification】Use show nfpp icmp-guard summary to view configuration information

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.36icmp-guard monitor-period

This command is used to configure monitoring time.

icmp-guard monitor-period seconds

Delete the monitoring time configuration and restore it to the Default Configuration.

no icmp-guard monitor-period

Restore Default Configuration.

default icmp-guard monitor-period

【Parameter Description】

Parameter	Description
seconds	Monitoring time, the unit is second, the value range is [180, 86400].

【Default Configuration】 The default value of the global monitoring time is 600 seconds.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】When an attacker is detected, if the isolation time is 0, the software will monitor the attacker, and the timeout is the monitoring time. During the software monitoring process, when the isolation time is configured as a non-zero value, the attackers monitored by the software will be automatically isolated, and the timeout is set as the isolation time. The monitoring time is only

meaningful when the isolation time is 0.

If the isolation time is changed from a non-zero value to zero, the attacker of the relevant port will be deleted directly instead of software monitoring.

【Configuration Example]】1: Configure the ICMP anti-attack monitoring time to 180 seconds.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# icmp-guard monitor-period 180
```

【Verification】Use show nfpp icmp-guard summary to view configuration information

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.37icmp-guard rate-limit

Configure the global speed limit waterline.

icmp-guard rate-limit { per-src-ip | per-port } pps

Delete the speed limit waterline configuration and restore to Default Configuration.

no icmp-guard rate-limit { per-src-ip | per-port }

Restore Default Configuration.

default icmp-guard rate-limit { per-src-ip | per-port }

【Parameter Description】

Parameter	Description
per-src-ip	Rate limiting per source IP address.
per-port	Speed limit on each port.
pps	The speed limit waterline value, the value range is [1,9999].

【Default Configuration】 See product feature document.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the ICMP anti-attack full speed limit waterline, based on the source IP speed limit waterline of 500pps, and based on the source port speed limit waterline of 800pps.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# icmp-guard rate-limit per-src-ip 500
AC-FS(config-nfpp)# icmp-guard rate-limit per-port 800
```

【Verification】Use show nfpp icmp-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.38 icmp-guard trusted-host

Configure trusted hosts that are not monitored.

icmp-guard trusted-host ip mask

Delete unmonitored trusted hosts.

no icmp-guard trusted-host { all | ip mask }

Clear Do not monitor trusted hosts.

default icmp-guard trusted-host

【Parameter Description】

Parameter	Description
ip	IP address.
mask	IP address mask.
all	Used with no to remove all trusted hosts configuration.

【Default Configuration】 By default, no trusted host is set.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】 If the administrator wants to not monitor a certain host, that is, express trust in the host, it can be configured through this command. The ICMP packets sent by the trusted host to the CPU will be allowed to be sent to the CPU without any speed limit and alarm processing. By configuring the mask, all hosts in a certain network segment can not be monitored.

A maximum of 500 trusted hosts can be set.

【Configuration Example]】1: Configure all hosts in the 1.1.1.0/24 network segment as ICMP anti-attack trusted hosts.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# icmp-guard trusted-host 1.1.1.0 255.255.255.0
```

【Verification】Use show nfpp icmp-guard trusted-host to view configuration information

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.39 ip-guard attack-threshold

Configure a global attack waterline, that is, when the packet speed exceeds the attack waterline, an attack is considered to exist.

ip-guard attack-threshold { per-src-ip | per-port } pps

Delete the attack waterline configuration and restore it to the Default Configuration.

no ip-guard attack-threshold { per-src-ip | per-port }

Restore Default Configuration.

default ip-guard attack-threshold { per-src-ip | per-port }

【Parameter Description】

Parameter	Description

per-src-ip	Configure the attack waterline for each source IP address.
per-port	Configure the attack waterline for each port.
pps	Attack waterline, the unit is the number of packets per second, and the value range is [1,9999].

【Default Configuration】 See the product feature document.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】 The attack waterline cannot be less than the speed limit waterline.

IP anti-scanning is aimed at IP packet attacks whose destination IP address is not the local IP address. For IP packets whose destination IP address is the local IP address, the rate is limited by CPP (CPU Protect Policy).

【Configuration Example]】 1: Configure IP anti-attack global attack waterline, the attack waterline based on source IP is 2pps, and the attack waterline based on source port is 50pps.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# ip-guard attack-threshold per-src-ip 2
AC-FS(config-nfpp)# ip-guard attack-threshold per-port 50
```

【Verification】 Use show nfpp ip-guard summary to view configuration information.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

4.40ip-guard enable

This command is used to globally enable the IP anti-scanning function.

ip-guard enable

Disable IP Anti-Scan.

no ip-guard enable

Restore Default Configuration.

default ip-guard enable

【Parameter Description】–

【Default Configuration】 The default IP anti-scanning function is enabled.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the global open IP anti-scan function.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# ip-guard enable
```

【Verification】Use show nfpp ip-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.41ip-guard isolate-period

This command is used to configure the global isolation time.

ip-guard isolate-period { seconds | permanent }

Delete the quarantine time configuration and restore to Default Configuration

no ip-guard isolate-period

Restore Default Configuration

default ip-guard isolate-period

【Parameter Description】

Parameter	Description
seconds	The isolation time, in seconds, in the range of 0 or [30, 86400].
permanent	permanent isolation.

【Default Configuration】 The default value of the global isolation time is 0, that is, no isolation.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the IP anti-attack global isolation time to 180 seconds.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# ip-guard isolate-period 180
```

【Verification】Use show nfpp ip-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.42 ip-guard monitored-host-limit

This command is used to configure the maximum number of monitored hosts supported.

ip-guard monitored-host-limit number

Delete the maximum number of monitored hosts configuration and restore to Default Configuration.

no ip-guard monitored-host-limit

Restore Default Configuration.

default ip-guard monitored-host-limit

【Parameter Description】

Parameter	Description
number	The maximum number of monitored hosts supported, ranging from 1 to 4294967295.

【Default Configuration】 The maximum number of monitored hosts is 1000 by default.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】 If the number of monitored hosts has reached the default 1000, and the administrator sets the maximum number of monitored hosts to less than 1000, the existing monitored hosts will not be deleted, but the message "%ERROR: The value that you configured is smaller than current monitored hosts 1000 (the number of monitored hosts configured), please clear a part of monitored hosts." to remind the administrator that the configuration does not take effect, and some hosts that have been monitored need to be deleted.

When the monitored host table is full, print the log "% NFPP_IP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 (configured monitored hosts) monitored hosts." to remind the administrator.

【Configuration Example]】 1: Configure the maximum number of monitored hosts for IP anti-attack to 200.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# ip-guard monitored-host-limit 200
```

【Verification】 Use show nfpp ip-guard summary to view configuration information.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

4.43 ip-guard monitor-period

This command is used to configure monitoring time.

ip-guard monitor-period seconds

Delete the monitoring time configuration and restore it to the Default Configuration.

no ip-guard monitor-period

Restore Default Configuration.

default ip-guard monitor-period

【Parameter Description】

Parameter	Description
seconds	Monitoring time, the unit is second, the value range is [180, 86400].

【Default Configuration】 The default value of monitoring time is 600 seconds.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】 When an attacker is detected, if the isolation time is 0, the software will monitor the attacker, and the timeout is the monitoring time. During the software monitoring process, when the isolation time is configured as a non-zero value, the attackers monitored by the software will be automatically isolated, and the timeout is set as the isolation time. The monitoring time is only meaningful when the isolation time is 0.

If the isolation time is changed from a non-zero value to zero, the attacker of the relevant port will be deleted directly instead of software monitoring.

【Configuration Example]】 1: Configure IP anti-attack monitoring time to 180 seconds.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# ip-guard monitor-period 180
```

【Verification】 Use show nfpp ip-guard summary to view configuration information.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】-

4.44ip-guard rate-limit

Configure global speed limit waterline.

ip-guard rate-limit { per-src-ip | per-port } pps

Delete the speed limit waterline configuration and restore to Default Configuration.

no ip-guard rate-limit { per-src-ip | per-port }

Restore Default Configuration.

default ip-guard rate-limit { per-src-ip | per-port }

【Parameter Description】

Parameter	Description
per-src-ip	Rate limiting per source IP address.
per-port	Speed limit on each port.
pps	The speed limit waterline value, the value range is [1,9999].

【Default Configuration】 See the product feature document.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the IP anti-attack full speed limit waterline, based on the source IP speed limit waterline 2pps, based on the source port speed limit waterline 50pps.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# ip-guard rate-limit per-src-ip 2
AC-FS(config-nfpp)# ip-guard rate-limit per-port 50
```

【Verification】Use show nfpp ip-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.45 ip-guard scan-threshold

Configure the global scan watermark.

ip-guard scan-threshold pkt-cnt

Delete the scan waterline configuration and restore to the Default Configuration

no ip-guard scan-threshold

Restore Default Configuration

default ip-guard scan-threshold

【Parameter Description】

Parameter	Description
pkt-cnt	Sweep waterline value, the value range is [1,9999].

【Default Configuration】 The default scanning watermark is 100 in 10 seconds.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the IP anti-attack full scan waterline to 20pps.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# ip-guard scan-threshold 20
```

【Verification】Use show nfpp ip-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.46 ip-guard trusted-host

If the administrator wants to not monitor a host, that is, to trust the host, it can be configured through this command.

ip-guard trusted-host ip mask

Delete unmonitored trusted hosts

no ip-guard trusted-host { all | ip mask }

Clear Do not monitor trusted hosts

default ip-guard trusted-host

【Parameter Description】

Parameter	Description
ip	IP address.
mask	IP address mask.
all	Used with no to remove all trusted hosts configuration.

【Default Configuration】-

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】 If the administrator wants to not monitor a certain host, that is, express trust in the host, it can be configured through this command. The IP packets sent by the trusted host to the CPU will be allowed to be sent to the CPU without any rate limit and alarm processing.

A maximum of 500 trusted hosts can be set.

【Configuration Example]】1: Configure all hosts in the 1.1.1.0/24 network segment as trusted hosts for IP attack resistance.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)#ip-guard trusted-host 1.1.1.0 255.255.255.0
```

【Verification】Use show nfpp ip-guard trusted-host to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.47 log-buffer entries

Configure the NFPP log buffer size.

log-buffer entries number

Delete the log buffer size configuration and revert to the Default Configuration.

no log-buffer entries

Restore Default Configuration.

default log-buffer entries

【Parameter Description】

Parameter	Description
number	Buffer size, the unit is the number of log entries, the value range is [0,1024].

【Default Configuration】 The default buffer size is 256.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the NFPP log buffer size to 50 logs.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# log-buffer entries 50
```

【Verification】Use show nfpp log summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.48 log-buffer logs

Configure the rate at which NFPP fetches logs from the log buffer to generate system messages.

log-buffer logs number_of_message interval length_in_seconds

Delete the rate configuration for generating system messages from the log buffer and restore it to the Default Configuration.

no log-buffer logs

Restore Default Configuration.

default log-buffer logs

【Parameter Description】

Parameter	Description
number_of_message	The range is 0-1024, 0 means that the log is all recorded in a dedicated buffer and no system messages are generated.
length_in_seconds	The range is 0-86400 (1 day), 0 means do not write the log to the buffer, but generate system messages immediately. Both number_of_message and length_in_seconds are 0 to not write the log to the buffer, but to generate system messages immediately. number_of_message /length_in_second indicates the rate at which the log generates system messages.

【Default Configuration】 The default value of number_of_message is 1, and the default value of length_in_seconds is 30.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the log generation rate to output 2 log messages every 12 seconds.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# log-buffer logs 2 interval 12
```

【Verification】Use show nfpp log summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.49 logging

Configure which VLANs or ports are logged by NFPP.

logging vlan vlan-range

logging interface interface-id

Delete the configuration of which VLANs or ports are logged by P

no logging vlan vlan-range

no logging interface interface-id

Restore Default Configuration.

default logging

【Parameter Description】

Parameter	Description
vlan-range	The log information in the specified VLAN range needs to be recorded. The input format is "1-3,5".
interface-id	The log information of the specified port needs to be recorded.

【Default Configuration】 All logs are recorded.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】 Through this command, you can filter the log, and only record the log information of the specified VLAN range or specified port. The relationship between the two log filtering configurations is OR, that is, only one of the log filtering rules needs to be satisfied, and it should be recorded in the log buffer.

【Configuration Example]】1: The administrator requests to record only the logs of VLAN 1, VLAN 2, VLAN 3 and VLAN 5. The configuration is as follows:

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# logging vlan 1-3,5
```

2: The administrator requires to record only the log of port G 0/1, the configuration is as follows:

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# logging interface G 0/1
```

【Verification】Use show nfpp log summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.50nd-guard attack-threshold

Configure a global attack waterline, that is, when the packet speed exceeds the attack waterline, an attack is considered to exist.

nd-guard attack-threshold per-port { ns-na | rs | ra-redirect } pps

Delete the attack waterline configuration and restore to Default Configuration.

no nd-guard attack-threshold per-port { ns-na | rs | ra-redirect }

Restore Default Configuration.

default nd-guard attack-threshold per-port { ns-na | rs | ra-redirect }

【Parameter Description】

Parameter	Description
ns-na	Neighbor Solicitation and Neighbor Advertisement.
rs	router request.
ra-redirect	Router Advertisement and Redirect Packets.
pps	Attack waterline, the unit is the number of packets per second, and the value range is [1,9999].

【Default Configuration】The default rate limit for each port neighbor solicitation/advertisement is 30 per second, the default rate limit for router requests is 30 per second, and the default rate limit for router advertisement/redirect packets is 30 per second.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】 The attack waterline cannot be less than the speed limit waterline.

【Configuration Example]】1: Configure the ND anti-attack global attack waterline, the source port-based ns-na attack waterline is 20pps, the source port-based rs attack waterline is 10pps, and the source port-based ra-redirect attack waterline is 10pps.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# nd-guard attack-threshold per-port ns-na 20 AC-
FS(config-nfpp)# nd-guard attack-threshold per-port rs 10 AC-FS(config-
nfpp)# nd-guard attack-threshold per-port ra-redirect 10
```

【Verification】Use show nfpp nd-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.51nd-guard enable

This command is used to enable ND anti-attack function globally.

nd-guard enable

Disable ND anti-attack function

no nd-guard enable

Restore Default Configuration

default nd-guard enable

【Parameter Description】-

【Default Configuration】 The default ND anti-attack function is enabled.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure to enable ND anti-attack function globally.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# nd-guard enable
```

【Verification】Use show nfpp nd-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.52nd-guard rate-limit

Configure the global speed limit waterline.

nd-guard rate-limit per-port { ns-na | rs | ra-redirect } pps

Delete the speed limit waterline configuration and restore to Default Configuration.

no nd-guard rate-limit per-port { ns-na | rs | ra-redirect }

Restore Default Configuration.

default nd-guard rate-limit per-port { ns-na | rs | ra-redirect }

【Parameter Description】

Parameter	Description
ns-na	Neighbor Solicitation and Neighbor Advertisement.
rs	router request.
ra-redirect	Router Advertisement and Redirect Packets.
pps	The speed limit waterline value, the value range is [1,9999].

【Default Configuration】 The default rate limit for each port neighbor solicitation/advertisement is 15 per second, the default attack threshold for router solicitation is 15 per second, and the default attack threshold for router advertisement/redirect packets is per second 15.

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the ND anti-attack full speed limit waterline, based on the source port ns-na speed limit waterline 10pps, based on the source port rs speed limit waterline 5pps, based on the source port ra-redirect speed limit waterline 5pps.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)# nd-guard rate-limit per-port ns-na 10 AC-
FS(config-nfpp)# nd-guard rate-limit per-port rs 5 AC-FS(config-
nfpp)# nd-guard rate-limit per-port ra-redirect 5
```

【Verification】Use show nfpp nd-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.53nd-guard trusted-host

If the administrator wants to not monitor a host, that is, to trust the host, it can be configured through this command.

nd-guard trusted-host mac

Delete unmonitored trusted hosts.

no nd-guard trusted-host { all | mac }

Clear Do not monitor trusted hosts.

default nd-guard trusted-host

【Parameter Description】

Parameter	Description
mac	MAC address.
all	Used with no to remove all trusted hosts configuration.

【Default Configuration】-

【Command Mode】 NFPP configuration mode

【Default Level】 14

【Usage Guide】 If the administrator wants to not monitor a certain host, that is, express trust in the host, it can be configured through this command. The ND packets sent by the trusted host to the CPU will be allowed to be sent to the CPU without any speed limit and alarm processing.

A maximum of 500 trusted hosts can be set.

【Configuration Example]】1: Configure the host whose MAC is 0000.0000.1111 as a trusted host for ND anti-attack.

```
AC-FS(config)# nfpp
AC-FS(config-nfpp)#nd-guard trusted-host 0000.0000.1111
```

【Verification】Use show nfpp nd-guard trusted-host to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.54nfpp arp-guard enable

This command is used to enable ARP anti-attack function on the port.

nfpp arp-guard enable

Disable the ARP anti-attack function on the port.

no nfpp arp-guard enable

Restore Default Configuration.

default nfpp arp-guard enable

【Parameter Description】–

【Default Configuration】 The port is not configured with the ARP anti-attack switch, and the global switch is used.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】The port's ARP anti-attack switch takes precedence over the global ARP anti-attack switch.

【Configuration Example】1 Enable ARP anti-attack and anti-attack capability on interface G0/1.

```
AC-FS(config)# interface G0/1
AC-FS(config-if)# nfpp arp-guard enable
```

【Verification】Use show nfpp nd-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.55nfpp arp-guard isolate-period

This command is used to configure the local isolation time on the port.

nfpp arp-guard isolate-period { seconds | permanent }

Delete the isolation time configuration on the port and restore it to the Default Configuration.

no nfpp arp-guard isolate-period

Restore Default Configuration.

default nfpp arp-guard isolate-period

【Parameter Description】

Parameter	Description
seconds	Isolation time, the unit is seconds, the value range is 0 or [30, 86400], 0 means no isolation.
permanent	permanent isolation.

【Default Configuration】 By default, the local isolation time is not configured, and the global isolation time is used.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the ARP anti-attack isolation time on interface G0/1 to 180 seconds.

```
AC-FS(config)# interface G 0/1
AC-FS(config-if)# nfpp arp-guard isolate-period 180
```

【Verification】Use show nfpp arp-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.56nfpp arp-guard policy

Configure the local rate limit watermark and attack watermark on the port.

nfpp arp-guard policy { per-src-ip | per-src-mac | per-port } rate-limit-pps attack-threshold-pps

Delete the port upper limit speed watermark and attack watermark configuration and restore to Default Configuration

no arp-guard policy { per-src-ip | per-src-mac | per-port }

Restore Default Configuration

default arp-guard policy { per-src-ip | per-src-mac | per-port }

【Parameter Description】

Parameter	Description
per-src-ip	Configure the rate limit watermark and attack watermark for each source IP address.
per-src-mac	Configure the rate limit watermark and attack watermark for each source MAC address.
per-port	Configure the rate limit watermark and attack watermark for each port.
rate-limit-pps	Speed limit watermark, the value range is 1 to 9999.
attack-threshold-pps	Attack waterline, the value range is 1 to 9999.

【Default Configuration】 The port does not have its own speed-limiting waterline and attack waterline, and adopts the global speed-limiting waterline and speed-limiting waterline.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 The attack waterline cannot be less than the speed limit waterline.

【Configuration Example]】1: Configure the ARP anti-attack speed limit waterline and attack waterline on interface G0/1, configure the

IP-based speed limit waterline of 2pps, and the attack waterline of 10pps; configure the MAC-based speed limit waterline of 3pps, and the attack waterline 10pps; the configuration is based on the port speed limit waterline of 50pps and the attack waterline of 100pps.

```
AC-FS(config)# interface G 0/1
AC-FS(config-if)# nfpp arp-guard policy per-src-ip 2 10
AC-FS(config-if)# nfpp arp-guard policy per-src-mac 3 10
AC-FS(config-if)# nfpp arp-guard policy per-port 50 100
```

【Verification】 Use show nfpp arp-guard summary to view configuration information.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

4.57nfpp arp-guard scan-threshold

Configure local scan watermarks on ports.

nfpp arp-guard scan-threshold pkt-cnt

Delete the scan watermark configuration on the port and restore it to the Default Configuration.

no nfpp arp-guard scan-threshold

Restore Default Configuration.

default nfpp arp-guard scan-threshold

【Parameter Description】

Parameter	Description
pkt-cnt	Sweep waterline value, the value range is [1,9999].

【Default Configuration】 The port-based ARP scan threshold is not configured, and the global ARP scan threshold is used.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the ARP anti-attack watermark on interface G0/1 to 20pps.

```
AC-FS(config)# interface G 0/1
AC-FS(config-if)# nfpp arp-guard scan-threshold 20
```

【Verification】Use show nfpp arp-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.58nfpp dhcp-guard enable

This command is used to enable DHCP anti-attack function on the port.

nfpp dhcp-guard enable

Disable DHCP anti-attack function on the port.

no nfpp dhcp-guard enable

Restore Default Configuration.

default nfpp dhcp-guard enable

【Parameter Description】–

【Default Configuration】 The port is not configured with the DHCP anti-attack switch, and the global switch is used.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 The port's DHCP anti-attack switch takes precedence over the global DHCP anti-attack switch.

【Configuration Example】1 Enable the anti-attack and anti-attack capability of DHCP on interface G0/1.

```
AC-FS(config)# interface G0/1
AC-FS(config-if)# nfpp dhcp-guard enable
```

【Verification】Use show nfpp dhcp-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.59nfpp dhcp-guard isolate-period

This command is used to configure the local isolation time on the port.

nfpp dhcp-guard isolate-period { seconds | permanent }

Delete the isolation time configuration on the port and restore it to the Default Configuration.

no nfpp dhcp-guard isolate-period

Restore Default Configuration.

default nfpp dhcp-guard isolate-period

【Parameter Description】

Parameter	Description
seconds	Isolation time, the unit is seconds, the value range is 0 or [30, 86400], 0 means no isolation.
permanent	permanent isolation.

【Default Configuration】 By default, the local isolation time is not configured, and the global isolation time is used.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the DHCP anti-attack isolation time on interface G0/1 to 180 seconds.

```
AC-FS(config)# interface G 0/1
AC-FS(config-if)# nfpp dhcp-guard isolate-period 180
```

【Verification】Use show nfpp dhcp-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.60nfpp dhcp-guard policy

Configure the local rate limit watermark and attack watermark on the port.

nfpp dhcp-guard policy { per-src-mac | per-port } rate-limit-pps attack-threshold-pps

Delete the port upper limit speed watermark and attack watermark configuration and restore to Default Configuration

no nfpp dhcp-guard policy { per-src-mac | per-port }

Restore Default Configuration

default nfpp dhcp-guard policy { per-src-mac | per-port }

【Parameter Description】

Parameter	Description
per-src-mac	Configure the rate limit watermark and attack watermark for each source MAC address.
per-port	Configure the rate limit watermark and attack watermark for each port.
rate-limit-pps	Speed limit watermark, the value range is 1 to 9999.
attack-threshold-pps	Attack waterline, the value range is 1 to 9999.

【Default Configuration】 The port does not have its own speed-limiting waterline and attack waterline, and adopts the global speed-limiting waterline and speed-limiting waterline.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 The attack waterline cannot be less than the speed limit waterline.

【Configuration Example]】1: Configure the DHCP anti-attack speed limit waterline and attack waterline on interface G0/1, configure the MAC-based speed limit waterline to 3pps, and configure the attack waterline to 10pps; configure the port-based speed limit waterline to 50pps, and the attack waterline 100pps.

```
AC-FS(config)# interface G 0/1
AC-FS(config-if)# nfpp dhcp-guard policy per-src-mac 3 10
AC-FS(config-if)# nfpp dhcp-guard policy per-port 50 100
```

【Verification】Use show nfpp dhcp-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.61nfpp dhcpv6-guard enable

This command is used to enable DHCPv6 anti-attack function on the port.

nfpp dhcpv6-guard enable

Disable DHCPv6 anti-attack function on port.

no nfpp dhcpv6-guard enable

Restore Default Configuration.

default nfpp dhcpv6-guard enable

【Parameter Description】–

【Default Configuration】 The port is not configured with the DHCPv6 anti-attack switch, and the global switch is used.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】The port's DHCPv6 anti-attack switch takes precedence over the global DHCP anti-attack switch.

【Configuration Example】1 Enable DHCPv6 anti-attack and anti-attack capability on interface G0/1.

```
AC-FS(config)# interface G0/1
AC-FS(config-if)# nfpp dhcpv6-guard enable
```

【Verification】Use show nfpp dhcpv6-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.62nfpp dhcpv6-guard isolate-period

This command is used to configure the local isolation time on the port.

nfpp dhcpv6-guard isolate-period { seconds | permanent }

Delete the isolation time configuration on the port and restore it to the Default Configuration.

no nfpp dhcpv6-guard isolate-period

Restore Default Configuration.

default nfpp dhcpv6-guard isolate-period

【Parameter Description】

Parameter	Description
seconds	Isolation time, the unit is seconds, the value range is 0 or [30, 86400], 0 means no isolation.
permanent	permanent isolation.

【Default Configuration】 By default, the local isolation time is not configured, and the global isolation time is used.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the DHCPv6 anti-attack isolation time on interface G0/1 to 180 seconds.

```
AC-FS(config)# interface G 0/1
AC-FS(config-if)# nfpp dhcpv6-guard isolate-period 180
```

【Verification】Use show nfpp dhcpv6-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.63nfpp dhcpv6-guard policy

Configure the local rate limit watermark and attack watermark on the port.

nfpp dhcpv6-guard policy { per-src-mac | per-port } rate-limit-pps attack-threshold-pps

Delete the port upper limit speed watermark and attack watermark configuration and restore to Default Configuration.

no nfpp dhcpv6-guard policy { per-src-mac | per-port }

Restore Default Configuration.

default nfpp dhcpv6-guard policy { per-src-mac | per-port }

【Parameter Description】

Parameter	Description
per-src-mac	Configure the rate limit watermark and attack watermark for each source MAC address.
per-port	Configure the rate limit watermark and attack watermark for each port.

rate-limit-pps	Speed limit watermark, the value range is 1 to 9999.
attack-threshold-pps	Attack waterline, the value range is 1 to 9999.

【 Default Configuration 】 The port does not have its own speed-limiting waterline and attack waterline, and adopts the global speed-limiting waterline and speed-limiting waterline.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 The attack waterline cannot be less than the speed limit waterline.

【Configuration Example]】 1: Configure the DHCP anti-attack speed limit watermark and attack watermark on interface G0/1, configure the IP-based speed limit waterline of 2pps and the attack waterline of 10pps; configure the MAC-based speed limit waterline of 3pps and the attack waterline 10pps; The configuration is based on the port speed limit waterline of 50pps and the attack waterline of 100pps.

```
AC-FS(config)# interface G 0/1
AC-FS(config-if)# nfpp dhcpv6-guard policy per-src-mac 3 10
AC-FS(config-if)# nfpp dhcpv6-guard policy per-port 50 100
```

【Verification】 Use show nfpp dhcpv6-guard summary to view configuration information.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

4.64nfpp icmp-guard enable

This command is used to enable the ICMP anti-attack function on the port.

nfpp icmp-guard enable

Turn off ICMP anti-attack on the port.

no nfpp icmp-guard enable

Restore Default Configuration.

default nfpp icmp-guard enable

【Parameter Description】–

【Default Configuration】 The port is not configured with the ICMP anti-attack switch, and the global switch is used.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】The ICMP anti-attack switch of the port takes precedence over the global ICMP anti-attack switch.

【Configuration Example】1 Enable ICMP anti-attack and anti-attack capability on interface G0/1.

```
AC-FS(config)# interface G0/1
AC-FS(config-if)# nfpp icmp-guard enable
```

【Verification】Use show nfpp icmp-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.65nfpp icmp-guard isolate-period

This command is used to configure the local isolation time on the port.

nfpp icmp-guard isolate-period { seconds | permanent }

Delete the isolation time configuration on the port and restore it to the Default Configuration.

no nfpp icmp-guard isolate-period

Restore Default Configuration.

default nfpp icmp-guard isolate-period

【Parameter Description】

Parameter	Description
seconds	Isolation time, the unit is seconds, the value range is 0 or [30, 86400], 0 means no isolation.
permanent	permanent isolation.

【Default Configuration】 By default, the local isolation time is not configured, and the global isolation time is used.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the ICMP anti-attack isolation time on interface G0/1 to 180 seconds.

```
AC-FS(config)# interface G 0/1
AC-FS(config-if)# nfpp icmp-guard isolate-period 180
```

【Verification】Use show nfpp icmp-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.66nfpp icmp-guard policy

Configure the local rate limit watermark and attack watermark on the port.

nfpp icmp-guard policy { per-src-ip | per-port } rate-limit-pps attack-threshold-pps

Delete the port upper limit speed watermark and attack watermark configuration and restore to Default Configuration.

no nfpp icmp-guard policy { per-src-ip | per-port }

Restore Default Configuration.

default nfpp icmp-guard policy { per-src-ip | per-port }

【Parameter Description】

Parameter	Description
per-src-ip	Configure the rate limit watermark and attack watermark for each source IP address.
per-port	Configure the rate limit watermark and attack watermark for each port.
rate-limit-pps	Speed limit watermark, the value range is 1 to 9999.
attack-threshold-pps	Attack waterline, the value range is 1 to 9999.

【Default Configuration】 The port does not have its own speed-limiting waterline and attack waterline, and adopts the global speed-limiting waterline and speed-limiting waterline.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 The attack waterline cannot be less than the speed limit waterline.

【Configuration Example]】1: Configure the ICMP anti-attack speed limit watermark and attack watermark on interface G0/1, configure the IP-based speed limit waterline of 5pps, and the attack waterline of 10pps; configure the port-based speed limit waterline of 100pps and the attack waterline 200pps.

```
AC-FS(config)# interface G 0/1
AC-FS(config-if)# nfpp icmp-guard policy per-src-ip 5 10
AC-FS(config-if)# nfpp icmp-guard policy per-port 100 200
```

【Verification】Use show nfpp icmp-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.67nfpp ip-guard enable

This command is used to enable the IP anti-scanning function on the port.

nfpp ip-guard enable

Turn off IP anti-scanning on a port.

no nfpp ip-guard enable

Restore Default Configuration.

default nfpp ip-guard enable

【Parameter Description】–

【Default Configuration】 The port is not configured with an IP anti-scanning switch, and a global switch is used.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 The IP anti-scanning switch of the port takes precedence over the global anti-scanning switch.

【Configuration Example】1 Enable the IP anti-scanning capability on interface G0/1.

```
AC-FS(config)# interface G0/1
AC-FS(config-if)# nfpp ip-guard enable
```

【Verification】Use show nfpp ip-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.68nfpp ip-guard isolate-period

This command is used to configure the local isolation time on the port.

nfpp ip-guard isolate-period { seconds | permanent }

Delete the isolation time configuration on the port and restore it to the Default Configuration.

no nfpp ip-guard isolate-period

Restore Default Configuration.

default nfpp ip-guard isolate-period

【Parameter Description】

Parameter	Description
seconds	Isolation time, the unit is seconds, the value range is 0 or [30, 86400], 0 means no isolation.
permanent	permanent isolation.

【Default Configuration】 By default, the local isolation time is not configured, and the global isolation time is used.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the IP anti-attack isolation time on interface G0/1 to 180 seconds.

```
AC-FS(config)# interface G 0/1
AC-FS(config-if)# nfpp ip-guard isolate-period 180
```

【Verification】Use show nfpp ip-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.69nfpp ip-guard policy

Configure the local rate limit watermark and attack watermark on the port.

nfpp ip-guard policy { per-src-ip | per-port } rate-limit-pps attack-threshold-pps

Delete the port upper limit speed watermark and attack watermark configuration and restore to Default Configuration.

no nfpp ip-guard policy { per-src-ip | per-port }

Restore Default Configuration.

default nfpp ip-guard policy { per-src-ip | per-port }

【Parameter Description】

Parameter	Description
per-src-ip	Configure the attack waterline for each source IP address.
per-port	Configure the attack waterline for each port.
rate-limit-pps	Speed limit watermark, the value range is 1 to 9999.
attack-threshold-pps	Attack waterline, the value range is 1 to 9999.

【Default Configuration】 The port does not have its own speed limit waterline and attack waterline, and adopts the global speed limit waterline and attack waterline.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 The attack waterline cannot be less than the speed limit waterline.

【Configuration Example】】 1: Configure the IP anti-attack speed limit waterline and attack waterline on interface G0/1, configure the IP-based speed limit waterline of 2pps and the attack waterline of 10pps; configure the port-based speed limit waterline of 50pps and the attack waterline 100pps.

```
AC-FS(config)# interface G 0/1
AC-FS(config-if)# nfpp ip-guard policy per-src-ip 2 10
AC-FS(config-if)# nfpp ip-guard policy per-port 50 100
```

【Verification】 Use show nfpp ip-guard summary to view configuration information.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】-

4.70nfpp ip-guard scan-threshold

Configure local scan watermarks on ports.

nfpp ip-guard scan-threshold pkt-cnt

Delete the scan watermark configuration on the port and restore it to the Default Configuration.

no nfpp ip-guard scan-threshold

Restore Default Configuration.

default nfpp ip-guard scan-threshold

【Parameter Description】

Parameter	Description
pkt-cnt	Sweep waterline value, the value range is [1,9999].

【Default Configuration】 The port-based IP scanning waterline is not configured, and the global ARP scanning waterline is used.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the IP anti-attack watermark on interface G0/1 to 20pps.

```
AC-FS(config)# interface G 0/1
AC-FS(config-if)# nfpp ip-guard scan-threshold 20
```

【Verification】Use show nfpp ip-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.71nfpp nd-guard enable

This command is used to enable ND anti-attack function on the port.

nfpp nd-guard enable

Disable the ND anti-attack function on the port.

no nfpp nd-guard enable

Restore Default Configuration.

default nfpp nd-guard enable

【Parameter Description】–

【Default Configuration】 The port is not configured with the ND anti-attack switch, and the global switch is used.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 The port's ND anti-attack switch takes precedence over the global switch.

【Configuration Example】1: Configure and enable ND anti-attack on port G0/1

```
AC-FS(config)# interface G0/1
AC-FS(config-if)# nfpp nd-guard enable
```

【Verification】Use show nfpp nd-guard summary to view configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

4.72nfpp nd-guard policy

Configure the local rate limit watermark and attack watermark on the port.

nfpp nd-guard policy per-port { ns-na | rs | ra-redirect } rate-limit-pps attack-threshold-pps

Delete the port upper limit speed watermark and attack watermark configuration and restore to Default Configuration

no nfpp nd-guard policy per-port { ns-na | rs | ra-redirect }

Restore Default Configuration

default nfpp nd-guard policy per-port { ns-na | rs | ra-redirect }

【Parameter Description】

Parameter	Description
ns-na	Neighbor Solicitation and Neighbor Advertisement.
rs	router request.
ra-redirect	Router Advertisement and Redirect Packets.
rate-limit-pps	Speed limit watermark, the value range is 1 to 9999.
attack-threshold-pps	Attack waterline, the value range is 1 to 9999.

【Default Configuration】 The port does not have its own speed limit waterline and attack waterline, and adopts the global speed limit waterline and attack waterline.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 The attack waterline cannot be less than the speed limit waterline.

ND snooping divides ports into untrusted ports and trusted ports. Untrusted ports connect to hosts, and trusted ports connect to gateways. Since the traffic of the trusted port is usually larger than that of the untrusted port, the speed limit watermark of the trusted port should be higher than the speed limit watermark of the untrusted port. When the ND snooping function is enabled, for the trusted port, ND snooping will notify the ND guard to The port's three types of packet rate limit waterlines are all set to 800 per second, and the attack waterlines are all set to 900 per second.

ND guard treats the speed limit waterline set by ND snooping and the speed limit waterline configured by the administrator equally. The value configured later overrides the value configured earlier, and is saved in the configuration file. The attack waterline set by ND snooping is similar.

【Configuration Example]】1: Configure the ND anti-attack rate limit watermark and attack watermark on interface G0/1, configure the port-based ns-na rate-limit watermark to 50pps and the attack waterline to 100pps; configure the port-rs-based rate limit watermark to

10pps , attack waterline 20pps; configuration based on port ra-redirect speed limit waterline 10pps, gongji waterline 20pps.

```
AC-FS(config)# interface G 0/1
AC-FS(config-if)# nfpp nd-guard policy per-port ns-na 50 100 AC-
FS(config-if)# nfpp nd-guard policy per-port rs 10 20 AC-FS(config-
if)# nfpp nd-guard policy per-port ra-redirect 10 20
```

【Verification】 Use show nfpp nd-guard summary to view configuration information.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

4.73 show nfpp arp-guard hosts

View monitored hosts.

show nfpp arp-guard hosts [statistics | [[vlan vid] [interface interface-id] [ip-address |

mac-address]]]

【Parameter Description】

Parameter	Description
statistics	View statistics for monitored hosts.
vid	Virtual LAN number.
interface-id	port name.
ip-address	IP address.
mac-address	MAC address.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example】】 1: View the statistics of ARP anti-attack monitored hosts. There are currently 120 hosts being monitored, of which 100 hosts were successfully quarantined and 20 hosts failed quarantine (usually due to insufficient memory, or insufficient ACL

resources).

```
AC-FS# show nfpp arp-guard hosts statistics
success  fail  total
_______   ____   _____
100       20      120
```

2: Check the ARP anti-attack monitored host, the fourth column "remain-time(s)" refers to the remaining isolation time.

```
AC-FS# show nfpp arp-guard hosts
If column 1 shows '*', it means "hardware do not isolate user" .
VLAN  interface IP address   MAC address      remain-time(s)
____  ________  _________    ___________      _____________
1      Gi0/1       1.1.1.1      -                  110
2      Gi0/2       1.1.2.1----------61
*3     Gi0/3       -              0000.0000.1111   110
4      Gi0/4       -              0000.0000.2222   61
Total: 4 hosts
```

【Prompt Information】-

【Platform Description】-

4.74 show nfpp arp-guard scan

View ARP scan table.

show nfpp arp-guard scan [statistics | [[vlan vid] [interface interface-id] [mac-address]]]

【Parameter Description】

Parameter	Description
statistics	View the number of records in the ARP scan table.
vid	Virtual LAN number.
interface-id	port name.
mac-address	MAC address.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: View ARP anti-attack scanning user statistics, the current scan table has a total of 4 records

```
AC-FS# show nfpp arp-guard scan statistics
ARP scan table has 4 record(s).
```

2: View ARP anti-attack scanning user information, "timestamp" records the time when ARP scanning was detected, such as "2008-01-23 16:23:10" means that an ARP scan was detected on January 23, 2008 at 16:23:10.

```
AC-FS# show nfpp arp-guard scan
VLAN    interface   IP address   MAC address      timestamp
____    ________    __________  ___________      __________
1        Gi0/1       N/A           0000.0000.0001   2008-01-23 16:23:10
2        Gi0/2.............1.1.1.1      0000.0000.0002   2008-01-23 16:24:10
3        Gi0/3       N/A           0000.0000.0003   2008-01-23 16:25:10
4        Gi0/4       N/A           0000.0000.0004 2008-01-23 16:26:10
Total: 4 record(s)
```

3: Only view the vlan 1, G0/1 port, which conforms to the scanning user information whose MAC is 0000.0000.0001.

AC-FS# show nfpp arp-guard scan vlan 1 interface G 0/1 0000.0000.0001

```
VLAN    interface   IP address   MAC address      timestamp
____    ________    __________    ___________      __________
1        Gi0/1       N/A            0000.0000.0001 2008-01-23 16:23:10
Total: 1 record(s)
```

【Prompt Information】-

【Platform Description】-

4.75show nfpp arp-guard summary

View configuration information.

show nfpp arp-guard summary

【Parameter Description】–

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to view configuration information.

【Configuration Example]】1: View the ARP anti-attack configuration information, including the global configuration information and the configuration information on the interface.

```
AC-FS# show nfpp arp-guard summary
 (Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface  Status  Isolate-period Rate-limit Attack-threshold Scan-threshold
Global      Enable  300             4/5/60     8/10/100           15
Gi 0/1       Enable  180             5/-/-       8/-/ ----------------------
Gi 0/2       Disable 200             4/5/60     8/10/100           20

Maximum count of monitored hosts: 1000
Monitor period: 300s
```

Field Interface is Global to indicate global configuration.

Field Status indicates whether the anti-attack function is enabled.

The format of Field Rate-limit is (rate limit watermark for source IP address/rate limit watermark for source MAC address/port rate limit watermark value).

Field Attack-threshold is displayed in a similar format. "-" means no configuration.

【Prompt Information】-

【Platform Description】-

4.76show nfpp arp-guard trusted-host

View trusted hosts that are not monitored.

show nfpp arp-guard trusted-host

【Parameter Description】–

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: View the ARP anti-attack trusted host configuration.

```
AC-FS# show nfpp arp-guard trusted-host
IP address      mac
---------       ------
1.1.1.1         0000.0000.1111

1.1.2.1         0000.0000.2222
Total: 2 record(s)
```

【Prompt Information】-

【Platform Description】-

4.77 show nfpp dhcp-guard hosts

View monitored hosts.

show nfpp dhcp-guard hosts [statistics | [[vlan vid] [interface interface-id] [mac-address]]]

【Parameter Description】

Parameter	Description
statistics	View statistics for monitored hosts.
vid	Virtual LAN number.
interface-id	port name.
mac-address	MAC address.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: View the statistics of DHCP anti-attack monitored hosts. There are currently 120 hosts being monitored, of which 100 hosts were successfully quarantined and 20 hosts failed quarantine (usually due to insufficient memory, or insufficient ACL resources).

```
AC-FS# show nfpp dhcp-guard hosts statistics
success  fail  total
-------  ----  -----
100         20        120
```

2: Check the DHCP anti-attack monitored host, the fourth column "remain-time(s)" refers to the remaining quarantine time.

```
AC-FS# show nfpp dhcp-guard hosts
If column 1 shows '*', it means "hardware failed to isolate host".
VLAN  interface MAC address  remain-time(seconds)
----  ---------  -----------        -----------------
 1     gi0/2      0000.0000.0001   10
 *2    gi0/1      0000.0000.0002 20
Total: 2 host(s)
```

【Prompt Information】-

【Platform Description】-

4.78 show nfpp dhcp-guard summary

View configuration information.

show nfpp dhcp-guard summary

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to view configuration information.

【Configuration Example]】1: View the DHCP anti-attack configuration information, including the global configuration information and the configuration information on the interface.

```
AC-FS# show nfpp dhcp-guard summary
 (Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface  Status  Isolate-period Rate-limit Attack-threshold
Global      Enable  300             -/5/150---------/10/300
Gi 0/1       Enable  180             -/6/------------ /8/-
Gi 0/2       Disable 200             -/5/30---------/10/50

Maximum count of monitored hosts: 1000
Monitor period: 300s
```

Field Interface is Global to indicate global configuration.

Field Status indicates whether the anti-attack function is enabled.

The format of Field Rate-limit is (rate limit watermark for source IP address/rate limit watermark for source MAC address/port rate limit watermark value).

Field Attack-threshold is displayed in a similar format. "-" means no configuration.

【Prompt Information】-

【Platform Description】-

4.79show nfpp dhcp-guard trusted-host

View trusted hosts that are not monitored.

show nfpp dhcp-guard trusted-host

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: View the DHCP anti-attack trusted host configuration.

```
AC-FS# show nfpp dhcp-guard trusted-host
mac
------

0000.0000.1111
0000.0000.2222
Total: 2 record(s)
```

【Prompt Information】-

【Platform Description】-

4.80 show nfpp dhcpv6-guard hosts

View monitored hosts.

show nfpp dhcpv6-guard hosts [statistics | [[vlan vid] [interface interface-id] [mac-address]]]

【Parameter Description】

Parameter	Description
statistics	View statistics for monitored hosts.
vid	Virtual LAN number.
interface-id	port name.
mac-address	MAC address.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: View the statistics of DHCPv6 anti-attack monitored hosts. There are currently 120 hosts being monitored, of which 100 hosts were successfully quarantined and 20 hosts failed quarantine (usually due to insufficient memory, or insufficient ACL resources).

```
AC-FS# show nfpp dhcpv6-guard hosts statistics
success  fail  total
-------  ----  -----

100         20        120
```

2: Check the DHCPv6 anti-attack monitored host, the fourth column "remain-time(s)" refers to the remaining quarantine time.

```
AC-FS# show nfpp dhcpv6-guard hosts
If column 1 shows '*', it means "hardware failed to isolate host".
VLAN  interface MAC address  remain-time(seconds)
----  ---------  -----------  -----------------
 1     gi0/2      0000.0000.0001   10
 *2    gi0/1      0000.0000.0002 20
Total: 2 host(s)
```

【Prompt Information】-

【Platform Description】-

4.81 show nfpp dhcpv6-guard summary

View configuration information.

show nfpp dhcpv6-guard summary

【Parameter Description】-

【Command Mode】 Privileged Mode

【Default Level】 14

【Usage Guide】 Use this command to view configuration information.

【Configuration Example]】1: View the DHCPv6 anti-attack configuration information, including the global configuration information and the configuration information on the interface.

```
AC-FS# show nfpp dhcpv6-guard summary
 (Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface  Status  Isolate-period Rate-limit Attack-threshold
Global      Enable  300             -/5/150---------/10/300
Gi 0/1       Enable  180             -/6/------------ /8/-
Gi 0/2       Disable 200             -/5/30---------/10/50

Maximum count of monitored hosts: 1000
Monitor period: 300s
```

Field Interface is Global to indicate global configuration.

Field Status indicates whether the anti-attack function is enabled.

The format of Field Rate-limit is (rate limit watermark for source IP address/rate limit watermark for source MAC address/port rate limit watermark value).

Field Attack-threshold is displayed in a similar format. "-" means no configuration.

【Prompt Information】-

【Platform Description】-

4.82 show nfpp dhcpv6-guard trusted-host

View trusted hosts that are not monitored.

show nfpp dhcpv6-guard trusted-host

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: View the DHCPv6 anti-attack trusted host configuration.

```
AC-FS# show nfpp dhcpv6-guard trusted-host
mac
------
0000.0000.1111
0000.0000.2222
Total: 2 record(s)
```

【Prompt Information】-

【Platform Description】-

4.83 show nfpp icmp-guard hosts

View monitored hosts.

show nfpp icmp-guard hosts [statistics | [[vlan vid] [interface interface-id] [ip-address]]]

【Parameter Description】

Parameter	Description
statistics	View statistics for monitored hosts.
vid	Virtual LAN number.
interface-id	port name.
ip-address	IP address.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: View the statistics of ICMP anti-attack monitored hosts. There are currently 120 hosts being monitored, of which 100 hosts were successfully quarantined and 20 hosts failed quarantine (usually due to insufficient memory, or insufficient ACL resources).

```
AC-FS#show nfpp icmp-guard hosts statistics
success  fail  total
_______    ____    _____
100         20        120
```

2: Check the ICMP anti-attack monitored host, the fourth column "remain-time(s)" refers to the remaining isolation time.

```
AC-FS#show nfpp icmp-guard hosts statistics
success  fail  total
_______    ____    _____
100         20        120
```

【Prompt Information】-

【Platform Description】-

4.84 show nfpp icmp-guard summary

View configuration information.

show nfpp icmp-guard summary

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to view configuration information.

【Configuration Example]】1: View the configuration information of ICMP anti-attack, including the global configuration information and the configuration information on the interface.

```
AC-FS# show nfpp icmp-guard summary
 (Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface  Status  Isolate-period Rate-limit Attack-threshold
Global       Enable  300              4/-/60      8/-/100
Gi 0/1        Enable  180               5/-/-        8/-/-
Gi 0/2  Disable 200  4/-/60  8/-/100

Maximum count of monitored hosts: 1000
Monitor period: 300s
```

Field Interface is Global to indicate global configuration.

Field Status indicates whether the anti-attack function is enabled.

The format of Field Rate-limit is (rate limit watermark for source IP address/rate limit watermark for source MAC address/port rate limit watermark value),

Field Attack-threshold is displayed in a similar format. "-" means no configuration.

【Prompt Information】-

【Platform Description】-

4.85 show nfpp icmp-guard trusted-host

View trusted hosts that are not monitored.

show nfpp icmp-guard trusted-host

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: View the ICMP anti-attack trusted host configuration.

```
AC-FS# show nfpp icmp-guard trusted-host
IP address      mask
————————        ————
1.1.1.0         255.255.255.0
1.1.2.0         255.255.255.0
Total: 2 record(s)
```

【Prompt Information】-

【Platform Description】-

4.86 show nfpp ip-guard hosts

View monitored hosts.

show nfpp ip-guard hosts [statistics | [[vlan vid] [interface interface-id] [ip-address]]]

【Parameter Description】

Parameter	Description
statistics	View statistics for monitored hosts.
vid	Virtual LAN number.
interface-id	port name.
ip-address	IP address.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: View the statistics of IP anti-attack monitored hosts. There are currently 120 hosts being monitored, of which 100 hosts were successfully quarantined and 20 hosts failed quarantine (usually due to insufficient memory, or insufficient ACL resources).

AC-FS#show nfpp ip-guard hosts statistics

```
success    fail    total
_______    ____    _____

100          20        120
```

2: Check the IP anti-attack monitored host, the fourth column "remain-time(s)" refers to the remaining isolation time.

```
AC-FS#show nfpp ip-guard hosts
If column 1 shows '*', it means "hardware do not isolate host".
VLAN  interface IP address   Reason      remain-time(s)
____  ________  _________    _______     ______________

1      Gi0/1       1.1.1.1      ATTACK      110
2      Gi0/2.....1.1.2.1      SCAN         61
Total: 2 host(s)
```

The fourth field "Reason" describes the reason why the host is being monitored, "ATTACK" indicates that the host sends IP packets faster than the attack waterline, and "SCAN" indicates that the host is scanning a certain network segment.

【Prompt Information】-

【Platform Description】-

4.87 show nfpp ip-guard summary

View configuration information.

show nfpp ip-guard summary

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to view configuration information.

【Configuration Example]】1: View the IP anti-attack configuration information, including the global configuration information and the configuration information on the interface.

```
AC-FS# show nfpp ip-guard summary
 (Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface Status Isolate-period Rate-limit Attack-threshold Scan-threshold
Global      Enable  300              4/-/60     8/-/100           15 Gi
0/1       Enable  180             5/-/-       8/-/ --------------------------
Gi 0/2       Disable 200             4/-/60     8/-/100           20

Maximum count of monitored hosts: 1000
Monitor period: 300s
```

Field Interface is Global to indicate global configuration.

Field Status indicates whether the anti-attack function is enabled.

The format of Field Rate-limit is (rate limit watermark for source IP address/rate limit watermark for source MAC address/port rate limit watermark value).

Field Attack-threshold is displayed in a similar format. "-" means no configuration.

【Prompt Information】-

【Platform Description】-

4.88 show nfpp ip-guard trusted-host

View trusted hosts that are not monitored.

show nfpp ip-guard trusted-host

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: View the IP anti-attack trusted host configuration.

```
AC-FS# show nfpp ip-guard trusted-host
IP address      mask
————————        ————
1.1.1.0         255.255.255.0
1.1.2.0         255.255.255.0
Total: 2 record(s)
```

【Prompt Information】-

【Platform Description】-

4.89 show nfpp log

Displays the NFPP log configuration.

show nfpp log summary

Displays the NFPP log buffer contents.

show nfpp log buffer [statistics]

【Parameter Description】

Parameter	Description
statistics	Display NFPP log buffer statistics.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 When the log buffer overflows, subsequent logs will be discarded, and an entry with all attributes of "-" will be displayed in the log buffer. Administrators need to increase the log buffer capacity or increase the rate at which system messages are generated. The system messages generated by fetching the log from the log buffer are timestamped with the occurrence of the event, as follows:

%NFPP_ARP_GUARD-4-DOS_DETECTED: Host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was detected.(2009-07-01 13:00:00)

【Configuration Example]】1: View the configuration of NFPP log information.

```
AC-FS#show nfpp log summary
Total log buffer size : 10
Syslog rate : 1 entry per 2 seconds
Logging:
VLAN  1-3, 5
interface Gi 0/1
interface Gi 0/2
```

2: Check the number of logs in the NFPP log buffer.

```
AC-FS#show nfpp log buffer statistics
There are 6 logs in buffer.
```

3: View the log buffer of NFPP.

```
AC-FS#show nfpp log buffer
Protocol VLAN  Interface IP address MAC address     Reason          Timestamp
-------- ----  --------- ---------- -------------   ------          ---------
ARP   1      Gi0/1       1.1.1.1---------- DoS              2009-05-30 16:23:10
ARP   1      Gi0/1       1.1.1.1       -              ISOLATED         2009-05-30 16:23:10
ARP   1      Gi0/1       1.1.1.2       -              DoS              2009-05-30 16:23:15
ARP   1      Gi0/1       1.1.1.2---------- ISOLATE_FAILED 2009-05-30 16:23:15
ARP   1      Gi0/1       -           0000.0000.0001  SCAN             2009-05-30 16:30:10
ARP   -      Gi0/2       -           -                 PORT_ATTACKED  2009-05-30 16:30:10
```

Protocol has the following values:

ARP	Corresponding to ARP anti-attack.
IP	Corresponding IP anti-scan.
ICMP	Corresponding to ICMP anti-attack.
DHCP	Corresponding to DHCP anti-attack.
DHCPv6	Corresponding to DHCPv6 anti-attack.
NS-NA	Corresponding to neighbor solicitation and neighbor advertisement in ND anti-attack.
RS	Corresponding to the router request in ND anti-attack.
RA-REDIRECT	Corresponding to router advertisement and redirection packets in ND anti-attack.

Reason represents the reason and has 5 values:

DoS	Indicates that a denial of service attack has been

	detected.
ISOLATED	Indicates that the attacker was successfully isolated.
ISOLATE_FAILED	Indicates failure to isolate attacker.
SCAN	Indicates that a scan was detected.
PORT_ATTACKED	Indicates that the port is attacked.

【Prompt Information】-

【Platform Description】-

4.90show nfpp nd-guard summary

View configuration information.

show nfpp nd-guard summary

【Parameter Description】-

【Command Mode】-

【Default Level】 14

【Usage Guide】 Use this command to view configuration information.

【Configuration Example]】1: View the ND anti-attack configuration information, including the global configuration information and the configuration information on the interface.

```
AC-FS# show nfpp nd-guard summary
 (Format of column Rate-limit and Attack-threshold is NS-NA/RS/RA-REDIRECT.)
Interface  Status  Rate-limit Attack-threshold
Global      Enable  20/5/10     40/10/20
Gi 0/1       Enable  15/15/15    30/30/30
Gi 0/2       Disable -/5/30----------/10/50
```

Field Interface is Global to indicate global configuration. Field Status indicates whether the anti-attack function is enabled.

The format of Field Rate-limit is (speed limit watermark for neighbor solicitation/advertisement/rate limit watermark for router request/rate limit watermark for router advertisement/redirect message), the display format of Field Attack-threshold similar. "-" means no configuration.

Example Description: "-/5/30" means that no neighbor solicitation/advertisement rate limit watermark is configured on port G 0/2, the rate limit watermark for router solicitation is 5, and the rate limit for router advertisement/redirect packets is 5. The speed limit is 30.

【Prompt Information】-

【Platform Description】-

4.91 show nfpp nd-guard trusted-host

View trusted hosts that are not monitored.

show nfpp nd-guard trusted-host

【Parameter Description】–

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: View the ND anti-attack trusted host configuration.

```
AC-FS# show nfpp nd-guard trusted-host
mac
------
0000.0000.1111
0000.0000.2222
Total: 2 record(s)
```

【Prompt Information】-

【Platform Description】-

Chapter 4 WLAN QOS

This volume introduces the relevant content of the WLAN QOS command manual, including the following chapters:

1. WQOS
2. WMM
3. VIP-FIRST

1 WQOS

1.1ap-based

Configure the upstream and downstream traffic rate limit parameters of the current AP.

ap-based { per-user-limit | total-user-limit } { down-streams | up-streams } average-data-rate

average-data-rate burst-data-rate burst-data-rate

Users can use the no option of this command to restore Parameter to the default value.

no ap-based { per-user-limit | total-user-limit } { down-streams | up-streams }

Configure the total-user-limit intelligent speed limit of the current AP.

ap-based total-user-limit { down-streams | up-streams } intelligent

The user can cancel the intelligent speed limit with the no option of this command.

no ap-based total-user-limit { down-streams | up-streams } intelligent

【Parameter Description】

Parameter	Description
per-user-limit	Rate limit for each user on the AP.
total-user-limit	Speed limit the entire AP.
down-streams	Indicates to set the downlink traffic rate limit parameter of the AP.
up-streams	Indicates that the upstream traffic rate limit parameter of the AP is set.
intelligent	Indicates whether to intelligently limit the total-user-limit.
average-data-rate	Indicates to set the average rate limit, the unit is 8Kbps, and the range is 8-261120.
burst-data-rate	Indicates to set the burst rate limit, the unit is 8Kbps, and the range is 8-261120.

【Default Configuration】 The default is no traffic rate limit. If total-user-limit is configured, intelligent speed limit is not enabled by default.

【Command Mode】 AP configuration mode.

【Default Level】15

【Usage Guide】The premise of enabling the smart speed limit is to configure the total-user-limit speed limit, otherwise the smart speed limit switch will not take effect.

【Configuration Example]】1: Set the average downlink rate of each user on AP wlan-ap-001 to 800KB/s and the burst rate to 1600KB/s.

```
AC-FS(config)# ap-config wlan-ap-001
AC-FS(config-ap)# ap-based per-user-limit down-streams average-data-rate 800 burst-data-rate 1600
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 AC

1.2 fair-schedule

Enable the fair scheduling function of the wireless AP.

fair-schedule

The user can disable this feature with the no option of this command.

no fair-schedule

【Parameter Description】 –

【Default Configuration】 It is enabled by default.

【Command Mode】 AP configuration mode

【Default Level】15

【Usage Guide】 When the AP works in thin AP mode, the fair scheduling function can only be configured on the AC.

【Configuration Example]】1: Disable the AP's fair scheduling function.

```
AC-FS(config)# ap-config ap-name
AC-FS(ap-config)# no fair-schedule
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.3 illegal-sta-check

Use illegal-sta-check to enable anti-proxy detection.

illegal-sta-check ip ttl

illegal-sta-check tcp source-ports [port-num]

Users can use the no command of this command to disable the anti-proxy detection function.

no illegal-sta-check ip ttl

no illegal-sta-check tcp source-ports

【Parameter Description】

Parameter	Description
port-num	Set the upper limit of the number of port detections, the range is 1 to 512, the default is 512.

【Default Configuration】 It is disabled by default.

【Command Mode】 AP configuration mode.

【Default Level】15

【Usage Guide】 None.

【Configuration Example]】1: Set ap1 to enable the anti-proxy detection function and use TTL as the policy.

```
AC-FS(config)# ap-config ap1
AC-FS(config-ap)#illegal-sta-check ip ttl
```

2: Set ap2 to enable the anti-proxy detection function, use source port detection as the policy, and the default port number is 512.

```
AC-FS(config)# ap-config ap2
AC-FS(config-ap)#illegal-sta-check tcp source-ports
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 AC, fat AP

1.4 netuser

Configure the upstream and downstream traffic rate limit Parameter based on the specified user.

netuser mac-address { inbound | outbound } average-data-rate average-data-rate burst-data-rate burst-data-rate

Users can use the no option of this command to restore Parameter to the default value.

no netuser mac-address { inbound | outbound }

【Parameter Description】

Parameter	Description
mac-address	Indicates the user's MAC address to be set.
inbound	Indicates setting the user's upstream traffic rate limit Parameter.
outbound	Indicates setting the user's downlink traffic rate limit Parameter.
average-data-rate	Indicates to set the average rate limit, the unit is 8Kbps, and the range is 8-261120.
burst-data-rate	Indicates to set the burst rate limit, the unit is 8Kbps, and the range is 8-261120.

【Default Configuration】 The default is no traffic rate limit.

【Command Mode】 AC configuration mode.

【Default Level】15

【Usage Guide】 None.

【Configuration Example]】1: Set the average uplink rate of user 0000.0000.0001 to 800KB/s and the burst rate to 1600KB/s.

```
AC-FS(config)# ac-controller
AC-FS(ac-config)# netuser 0000.0000.0001 inbound average-data-rate 800 burst-data-rate 1600
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.5show dot11 ratelimit

Displays the speed limit information of the WLAN.

show dot11 ratelimit { wlan | ap | user }

show dot11 ratelimit wlan per-ap

【Parameter Description】

Parameter	Description
wlan	Indicates that the speed limit information of all WLANs is displayed.
ap	Indicates that the speed limit information of all APs is displayed.
user	Indicates that the speed limit information of all users is displayed.
per-ap	Indicates the wlan total speed limit of all APs.

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】 None.

【Configuration Example】1: Display the speed limit information of all APs.

```
AC-FS# show dot11 ratelimit ap
```

【Prompt Information】-

【Platform Description】-

1.6sta-fair

Configure the fair scheduling priority of the specified user.

sta-fair mac-address priority priority

Users can use the no command of this command to restore Parameter to the default value.

no sta-fair mac-address

【Parameter Description】

Parameter	Description
mac-address	Indicates the user's MAC address to be set.
priority	A numeric value representing the priority, in the range 1-6.

【Default Configuration】 The default priority of all STAs is 1.

【Command Mode】 AC configuration mode.

【Default Level】15

【Usage Guide】 None.

【Configuration Example]】1: Set the fair scheduling priority of user 0000.0000.0001 to 3 on the ac

```
AC-FS(config)# ac-controller
AC-FS(config-ac)# sta-fair 0000.0000.0001 priority 3
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.7wlan-based

Configure the upstream and downstream traffic rate limit parameters of the current WLAN.

wlan-based { per-user-limit | total-user-limit | per-ap-limit } { down-streams | up-streams }

average-data-rate average-data-rate burst-data-rate burst-data-rate

Users can use the no option of this command to restore Parameter to the default value.

no wlan-based { per-user-limit | total-user-limit | per-ap-limit } { down-streams | up-streams }

Configure the per-ap-limit intelligent speed limit of the current WLAN.

wlan-based per-ap-limit { down-streams | up-streams } intelligent

The user can cancel the intelligent speed limit with the no option of this command.

no wlan-based per-ap-limit { down-streams | up-streams } intelligent

【Parameter Description】

Parameter	Description
per-user-limit	Rate limit per user on the WLAN.
total-user-limit	Speed limit the entire WLAN.
per-ap-limit	Do WLAN TOTAL speed limit for each AP individually.
down-streams	Indicates setting the WLAN downlink traffic rate limit Parameter.
up-streams	Indicates setting the WLAN upstream traffic rate limit Parameter.
intelligent	Indicates whether to intelligently limit the per-ap-limit.
average-data-rate	Indicates to set the average rate limit, the unit is 8Kbps, and the range is 8-261120.
burst-data-rate	Indicates to set the burst rate limit, the unit is 8Kbps, and the range is 8-261120.

【Default Configuration】 The default is no traffic rate limit. If per-ap-limit is configured, intelligent speed limit is not enabled by default.

【Command Mode】 WLAN configuration mode.

【Default Level】15

【Usage Guide】The premise of enabling the smart speed limit is to configure the per-ap-limit speed limit, otherwise the smart speed limit switch alone will not take effect.

【Configuration Example]】1: Set the average downlink rate of each user on WLAN 1 to 800KB/s and the burst rate to 1600KB/s.

```
AC-FS(config)# wlan-config 1
AC-FS(config-ap)# wlan-based per-user-limit down-streams average-data-rate 800 burst-data-rate
1600
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.8wqos fs enable

Enable the wqos traffic statistics function.

wqos fs enable

Disable the wqos traffic statistics function.

no wqos fs enable

【Parameter Description】–

【Default Configuration】 By default, the wqos traffic statistics function is disabled.

【Command Mode】AC configuration mode

【Default Level】15

【Usage Guide】 This command is used to supplement the non-WEB authentication/1X authentication environment and enable the wqos traffic statistics function. If WEB authentication/1X authentication has been configured, the wqos traffic statistics function is enabled by default, so it is invalid to enable or disable the wqos traffic statistics function through this command.

【Configuration Example]】1: All APs associated with the AC are enabled to enable the WQOS traffic statistics function.

```
AC-FS(config-ac)#wqos fs enable
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2 WMM

2.1 wlan-qos map-table

Configure the packet priority mapping relationship of the current WLAN.

wlan-qos map-table { dot11e-inner-dscp | dot11e-tunnel-dscp | dscp-dot11e } import import-tag-value export export-tag-value

Restore the packet priority mapping relationship of the default WLAN.

no wlan-qos map-table { dot11e-inner-dscp | dot11e-tunnel-dscp | dscp-dot11e } import import-tag-value

【Parameter Description】

Parameter	Description
dot11e-inner-dscp	Sets priority mapping from dot11e to internal DSCP.
dot11e-tunnel-dscp	Sets priority mapping from dot11e to CAPWAP DSCP.
dscp-dot11e	Sets priority mapping from DSCP to dot11e.
import import-tag-value	Sets priority of the incoming original packet. WMM (dot11e) is one of QoS fields of 802.11 wireless protocol headers. It refers to WLAN priority, in the range from 0 to 7. DSCP is the priority field of IP protocol headers, in the range from 0 to 63. The default is 0.
export export-tag-value	Indicates to set the priority of output packets. WMM(dot11e)--a part of the QOS Field in the 802.11 wireless protocol header, indicating the wireless priority, the value range is 0-7; dscp-- is the priority Field in the IP protocol header, the value range is 0-63, the default value is 0.
no	Indicates that the restored packet mapping relationship is the default value.

【Default Configuration】 DSCP-to-dot11e Mapping Table.

DSCP	802.11e
0~7	0
16~23	1
24~31	2
8~15	3
32~39	4

40~47	5
48~55	6
56~63	7

Dot11e-to-DSCP Mapping Table

802.11e	DSCP
0	0
3	8
1	16
2	24
4	32
5	40

【Command Mode】 WLAN configuration mode

【Default Level】 14

【Usage Guide】 This command is a non-interoperable version mapping command.

The configuration takes effect only when the wmm service is enabled.

【Configuration Example】 The following example sets priority mapping from DSCP to dot11e. The priority of the incoming original packet is 1 and that of the outgoing packet is 10.

```
AC-FS# configure terminal AC-
FS(config)# wlan-config 1
AC-FS(config-wlan)# wlan-qos map-table dscp-dot11e import 1 export 10
```

【Verification】 1: Use the show run command to view the currently effective priority mapping, which is not displayed in the default configuration.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

2.2 wmm dot1p enable

Enable 802.11p QoS mapping policy mechanism.

wmm dot1p enable radio radio-id

Turn off the 802.11p QoS mapping policy mechanism.

no wmm dot1p enable radio radio-id

【Parameter Description】

Parameter	Description
radio radio-id	Indicates the radio that selects to enable/disable the 802.11p QoS mapping policy mechanism, the range is 1-96.
no	no means to restore the default configuration.

【Default Configuration】 The default is to disable the 802.11p QoS mapping policy mechanism.

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 This command is the interworking version mapping command.

The configuration takes effect only when the wmm service is enabled.

【Configuration Example】 The following example enables 802.11p QoS mapping policy mechanism for radio 1 on VOICE-AP.

```
AC-FS# configure terminal AC-
FS(config)# ap-config VOICE-AP
AC-FS(config-ap)# wmm dot1p enable radio 1
```

【Verification】 1: Use the show running or show ap-config running command to check whether the 802.11p QoS mapping policy is enabled. It is not displayed in the default configuration.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

2.3 wmm dot1p policy

Configure how the AP applies the 802.11p QoS mapping policy mechanism.

wmm dot1p policy 1q [1q-policy-value] radio radio-id

Restores how the default AP applies the 802.11p QoS mapping policy mechanism.

no wmm dot1p policy radio radio-id

【Parameter Description】

Parameter	Description
1q1q-policy-value	Applies the 802.11p QoS mapping policy mechanism, in the range from 0 to 1. The default is 0. Q=1: AP tags the priority domain of 802.1Q according to 802.1p. Q=0: AP tags the priority domain of 802.1Q according to the user priority in the Qos Control field of IEEE 802.11 headers. Apply "Q=1" method when there is no QoS Control field.
radio radio-id	The radio that indicates how the AP applies the 802.11p QoS mapping policy mechanism, the range is 1-96.
no	no means to restore the default configuration

【Default Configuration】 The default configuration is 0.

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 This command is the interworking version mapping command.

The configuration takes effect only when the wmm service is enabled.

When the 802.11p QoS mechanism is enabled, the configuration and application of the 802.11p QoS mapping policy mechanism is valid.

【Configuration Example】 1: Set radio 1 of VOICE-AP to mark the priority field in the 802.1Q header according to the delivered 802.1p.

```
AC-FS# configure terminal AC-
FS(config)# ap-config VOICE-AP
AC-FS(config-ap)# wmm dot1p 1q 1 radio 1
```

【Verification】 1: Use show running or show ap-config running to view the currently applied 802.11p QoS mapping policy mechanism,

which is not displayed in the default configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.3 wmm dot1p tag

Configure 802.1p priority.

wmm dot1p tag [tag-value] { back-ground | best-effort | video | voice } radio radio-id

Restore default 802.1p priority.

no wmm dot1p tag { back-ground | best-effort | video | voice } radio radio-id

【Parameter Description】

Parameter	Description
tag tag-value	Indicates to set the 802.1p priority, the range is 0-7, the default value of best-effort is 0, the default value of background-ground is 2, the default value of video is 4, and the default value of voice is 6.
back-ground	Indicates that the background queue will be set.
best-effort	Indicates that the best-effort queue will be set.
video	Indicates that the video queue will be set.
voice	Indicates that the voice queue will be set.
radio radio-id	Indicates the radio to set the 802.1p priority, the range is 1-96.
no	no means to restore the default configuration.

【Default Configuration】The default value of best-effort is 0, the default value of back-ground is 2, the default value of video is 4, and the default value of voice is 6.

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 This command is the interworking version mapping command.

The configuration takes effect only when the wmm service is enabled.

The 802.1p priority is only valid when the 802.11p QoS mechanism is enabled.

【Configuration Example】 1: Set the 802.1p priority of the voice queue under radio 1 of VOICE-AP to 5.

```
AC-FS# configure terminal AC-
FS(config)# ap-config VOICE-AP
AC-FS(config-ap)# wmm dot1p tag 5 voice radio 1
```

【Verification】 1: Use show running or show ap-config running to view the 802.1p priority, which is not displayed in the default configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.4 wmm dscp enable

Enable dscp QoS mapping policy mechanism.

wmm dscp enable radio radio-id

Turn off the dscp QoS mapping policy mechanism.

no wmm dscp enable radio radio-id

【Parameter Description】

Parameter	Description
radio radio-id	Indicates the radio that selects to enable/disable the dscp QoS mapping policy mechanism, the range is 1-96.
no	no means to restore the default configuration.

【Default Configuration】 The default is to disable the dscp QoS policy mechanism.

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 This command is the interworking version mapping command.

The configuration takes effect only when the wmm service is enabled.

【Configuration Example】 The following example enables DSCP QoS mapping policy mechanism for radio 1 on VOICE-AP.

```
AC-FS# configure terminal AC-
FS(config)# ap-config VOICE-AP
AC-FS(config-ap)# wmm dscp enable radio 1
```

【Verification】1: Use show running or show ap-config running to check whether the dscp QoS mapping policy is enabled. It is not displayed in the default configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.5 wmm dscp policy

Configure how the AP applies the dscp QoS mapping policy mechanism.

wmm dscp policy outer-tunnel [outer-tunnel-value] inner-tunnel [inner-tunnel-value] radio radio-id

Restores how the default AP applies the dscp QoS mapping policy mechanism.

no wmm dscp policy radio radio-id

【Parameter Description】

Parameter	Description
outer-tunnel outer-tunnel-value	Configures how to apply the DSCP QoS mapping policy mechanism for the outer tunnel header, in the range from 0 to 1. The default is 0. In the centralized forwarding mode: O=1: AP sets DSCP domain for the tunnel header according to pushed configuration policy; O=0: AP sets DSCP domain for the tunnel header according to inner tunnel packets. If inner tunnel packets are encrypted or non-IPv4, the "O=1" method will be applied. In the local forwarding mode: O=1: invalid value; O=0: invalid value.
	Configures how to apply the DSCP QoS mapping policy mechanism for the inner

inner-tunnel inner-tunnel-value	tunnel header, in the range from 0 to1. The default is 0. In the centralized forwarding mode: AP sets DSCP domain for the tunnel header according to inner tunnel packets; If inner tunnel packets are encrypted or non-IPv4, the "I=1" method will be applied. I=0: AP cannot modify the DSCP domain of user packets. In the local forwarding mode: I=1: AP configures the DSCP domain for user packets according to the pushed
radio radio-id	The radio that indicates how the AP applies the dscp QoS mapping policy mechanism, the range is 1-96.
no	no means to restore the default configuration.

【Default Configuration】 The default configuration is 0.

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 This command is the interworking version mapping command.

The configuration takes effect only when the wmm service is enabled.

When the dscp QoS mechanism is enabled, the configuration and application of the dscp QoS mapping policy mechanism is valid.

【Configuration Example】 1: Set the dscp mapping policy mechanism of the VOICE-AP radio 1 to 0 for the outer tunnel header and 0 for the inner tunnel header.

```
AC-FS# configure terminal AC-
FS(config)# ap-config VOICE-AP
AC-FS(config-ap)# wmm dscp outer-tunnel 0 inner-tunnel 0 radio 1
```

【Verification】1: Use show running or show ap-config running to view the currently applied dscp QoS mapping policy mechanism, which is not displayed in the default configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.6 wmm dscp tag

Configure the dscp identity.

wmm dscp tag [tag-value] { back-ground | best-effort | video | voice } radio radio-id

Restore the default dscp identity.

no wmm dscp tag { back-ground | best-effort | video | voice } radio radio-id

【Parameter Description】

Parameter	Description
tag tag-value	Indicates to set the dscp priority, the range is 0-63, the default value of best-effort is 0, the default value of background-ground is 16, the default value of video is 32, and the default value of voice is 48.
back-ground	Indicates that the background queue will be set.
best-effort	Indicates that the best-effort queue will be set.
video	Indicates that the video queue will be set.
voice	Indicates that the voice queue will be set.
radio radio-id	Indicates to select the radio whose dscp ID is set, the range is 1-96.
no	no means to restore the default configuration.

【Default Configuration】 The default value of best-effort is 0, the default value of back-ground is 16, the default value of video is 32, and the default value of voice is 48.

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 This command is the interworking version mapping command.

The configuration takes effect only when the wmm service is enabled.

The dscp identifier is only valid when the dscp mechanism is enabled.

【Configuration Example】 1: Set the dscp ID of the voice queue under radio 1 of VOICE-AP to 5.

```
AC-FS# configure terminal AC-
FS(config)# ap-config VOICE-AP
AC-FS(config-ap)# wmm dscp tag 5 voice radio 1
```

【Verification】1: Use show running or show ap-config running to view the dscp logo, which is not displayed in the default configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.7 wmm edca-client

Configure the client's EDCA Parameter.

wmm edca-client { back-ground | best-effort | video | voice } { aifsn [aifsn-value] cwmin [cwmin-value]

cwmax [cwmax-value] txop [txop-value] | length [queue-length] } radio radio-id

Restore the client default EDCA Parameter.

no wmm edca-client { back-ground | best-effort | video | voice } [length] radio radio-id

【Parameter Description】

Parameter	Description
back-ground	Indicates that the background queue will be set.
best-effort	Indicates that the best-effort queue will be set.
video	Indicates that the video queue will be set.
voice	Indicates that the voice queue will be set.
aifsn aifsn-value	Indicates to set the aifsn value, the range is 1-15.
cwmin cwmin-value	Indicates to set the cwmin value, the range is 0-15.
cwmax cwmax-value	Indicates to set the cwmax value, the range is 0-15.
txop txop-value	Indicates to set the txop value, the range is 0-255, and the unit is 32 microseconds.
length queue-length	Indicates to set the AC queue length, the range is 1-255. Defaults to the maximum value.
radio radio-id	Indicates the radio that selects to set the client EDCA Parameter, the range is 1-96.
no	no means to restore the default configuration.

【Default Configuration】

AC	aifs	cwmin	cwmax	txop

back-ground	7	4	10	0
best-effort	3	4	10	0
video	2	3	4	94
voice	2	2	3	47

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 The configured Parameter can take effect only when the wmm service is enabled.

The cwmax value must be greater than the cwmin value. Otherwise, it will prompt configuration failure.

【Configuration Example】1: Set the client's voice queue EDCA Parameter under radio 1 of VOICE-AP to aifsn 2 cwmin 2 cwmax 3 txop 50.

```
AC-FS# configure terminal AC-
FS(config)# ap-config VOICE-AP
AC-FS(config-ap)# wmm edca-client voice aifsn 2 cwmin 2 cwmax 3 txop 50 radio 1
```

【Verification】1: Use show running or show ap-config running to view the EDCA Parameter of the currently effective client, which is not displayed in the default configuration.

【Prompt Information】 1: If the radio does not exist, it will prompt an error.

```
This radio is not exist.
```

2: If the cwmax value is less than the cwmin value, an error will be prompted.

```
Cwmax must be greater than cwmin!
```

【Common Mistake】 1: When the EDCA Parameter configuration is unreasonable, the performance will be affected. For example, a configuration parameter with a low priority is better than a configuration parameter with a high priority, which affects the performance of the high priority.

【Platform Description】-

2.8 wmm edca-radio

Configure the EDCA Parameter used by the AP.

wmm edca-radio { back-ground | best-effort | video | voice } { aifsn [aifsn-value] cwmin [cwmin-value]

cwmax [cwmax-value] txop [txop-value] | noack } radio radio-id

Restore the default EDCA Parameter used by the AP.

no wmm edca-radio { back-groud | best-effort | video | voice } [noack] radio radio-id

【Parameter Description】

Parameter	Description
back-ground	Indicates that the background queue will be set.
best-effort	Indicates that the best-effort queue will be set.
video	Indicates that the video queue will be set.
voice	Indicates that the voice queue will be set.
aifsn aifsn-value	Indicates to set the aifsn value, the range is 1-15.
cwmin cwmin-value	Indicates to set the cwmin value, the range is 0-15.
cwmax cwmax-value	Indicates to set the cwmax value, the range is 0-15.
txop txop-value	Indicates to set the txop value, the range is 0-255 and the unit is 32 microseconds.
noack	Indicates that the no ack policy is enabled. The no ack policy is not enabled by default.
radio radio-id	Indicates the radio that selects to set the EDCA Parameter used by the AP, the range is 1-96.
no	no means to restore the default configuration.

【Default Configuration】

AC	aifs	cwmin	cwmax	txop
back-ground	7	4	10	0
best-effort	3	4	6	0
video	1	3	4	94
voice	1	2	3	47

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 The configured Parameter can take effect only when the wmm service is enabled.

According to the IEEE 802.11 standard, no ACK is returned for multicast or broadcast frames.

The cwmax value must be greater than the cwmin value. Otherwise, it will prompt configuration failure.

【Configuration Example】 The following example sets aifsn to 1, cwmin to 1, cwmax to 3, txop to 50 for the voice queue of radio 1 on

VOICE-AP.

```
AC-FS# configure terminal AC-
FS(config)# ap-config VOICE-AP
AC-FS(config-ap)# wmm edca-radio voice aifsn 1 cwmin 1 cwmax 3 txop 50 radio 1
```

【Verification】1: Use show running or show ap-config running to view the EDCA Parameter used by the currently valid AP, which is not displayed in the default configuration.

【Prompt Information】 1: If the radio does not exist, it will prompt an error.

```
This radio is not exist.
```

2: If the Parameter setting is wrong, it will prompt an error.

```
Cwmax must be greater than cwmin!
```

【Common Mistake】 1: When the EDCA Parameter configuration is unreasonable, the performance will be affected. For example, a configuration parameter with a low priority is better than a configuration parameter with a high priority, which affects the performance of the high priority.

【Platform Description】-

2.9 wmm enable

Configure the AP to enable the WMM service.

wmm enable radio radio-id

Disable the WMM service on the configuration AP.

no wmm enable radio radio-id

【Parameter Description】

Parameter	Description
radio radio-id	Indicates the radio that selects to enable/disable the WMM service, the range is 1-96.
no	no means off.

【Default Configuration】 The WMM service is enabled by default.

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 The wmm service is closed, and the default priority queue is used to receive and map.

【Configuration Example】 The following example enables the WMM service for radio 1 on VOICE-AP.

```
AC-FS# configure terminal AC-
FS(config)# ap-config VOICE-AP
AC-FS(config-ap)# wmm enable radio 1
```

【Verification】1: Use show running or show ap-config running to check whether the current wmm service is enabled. It is not displayed in the default configuration.

【Prompt Information】 1: If the radio does not exist, it will prompt an error.

```
This radio is not exist.
```

【Common Mistake】-

【Platform Description】-

3 VIP-FIRST

3.1 vip-first clear

Notify the AC to delete the VIP user list

vip-first clear

The command is not saved and does not provide a no mechanism

【Parameter Description】-

【Default Configuration】 N/A

【Command Mode】 AC Global configuration mode.

【Default Level】 15

【Usage Guide】 None

【Configuration Example】 Notify the AC to delete the VIP user list.

```
AC-FS(config)# vip-first clear
```

【Verification】 -

【Prompt Information】-

【Common Mistake】 -

【Platform Description】 AC

3.2 vip-first import

Notify the AC to resolve the VIP user list.

vip-first import

The command is not saved and does not provide a no mechanism.

【Parameter Description】-

【Default Configuration】 N/A

【Command Mode】 AC Global configuration mode

【Default Level】 15

【Usage Guide】 First upload the VIP user list file vip_user_list.txt to the AC's flash: Under the path, then execute the import command. The VIP user list file name is fixed to vip_user_list.txt

The vip_user_list.txt content format is: each line starts with a user MAC address, one MAC address per row, and each line ends with a return key.

For example: 0000.0000.0001, 0000.0000.0002

【Configuration Example】 Configuration Notification AC to resolve the VIP user list.

```
AC-FS(config)# vip-first import
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 Execute the import command without uploading the VIP user list file.

【Platform Description】 AC

3.3 vip-first prior-assoc

Turn on the vip-first priority access function.

vip-first prior-assoc

Users can use the no command to turn off the vip-first priority access feature.

no vip-first prior-assoc

【Parameter Description】 -

【Default Configuration】 Default closed.

【Command Mode】 AC Global configuration mode.

【Default Level】 15

【Usage Guide】 N/A

【Configuration Example】 Configure the vip-first priority access feature on.

```
AC-FS(config)# vip-first prior-assoc
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 AC

3.4 vip-first rate-limit

Configure the upward and downlink traffic speed limit parameters for VIP users.

Turn on the vip-first independent speed limit function

vip-first rate-limit { **up-stream** | **down-stream** } **average-rate** *average-rate* **burst-rate** *burst-rate*

The user can turn this function off with the no option of this command

no vip-first rate-limit { up-stream | down-stream }

【Parameter Description】

Parameter	Description
up-stream	Indicates the set user's upward flow speed limit parameter.
down-stream	Indicates the downlink traffic speed limit parameter for setting the user.
average-rate	Indicates setting the average rate limit in 8Kbps, in the range 8 – 261120.
burst-rate	Indicates setting a burst rate limit in 8Kbps, in the range of 8-261120.

【Default Configuration】 The default is the traffic speed limit for no VIP users. No vip-first independent speed limit function is turned on.

【Command Mode】 AC Global configuration mode

【Default Level】 15

【Usage Guide】 N/A

【Configuration Example】 Set the average upside rate for VIP user users to 800 Kb/s and a burst rate of 1600Kb / s.

```
AC-FS(config)# vip-first rate-limit up-stream average-rate 100 burst-rate 200
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 No global speed limit is configured, only the VIP user independent speed limit configuration.

【Platform Description】 AC

3.5 show vip-first user [mac]

See if the user is a VIP user

show vip-first user [mac]

【Parameter Description】

Parameter	Description
mac	Represents the mac address of the user.

【Command Mode】 Privilege mode

【Default Level】 1

【Usage Guide】 N/A

【Configuration Example】 Check out if 0000.0000.0001 is a VIP user.

```
AC-FS# show vip-first user 0000.0000.0001
STA_MAC        YES/NO

_____________  _____
0000.0000.0001 YES
```

【Prompt Information】 -

【Platform Description】 AC

Chapter 5 WLAN networking

This volume introduces the relevant contents of WLAN networking command manual, including the following chapters:

1. WDS

1 WDS

1.1 autowds

Configure the automatic bridging function of the AP partners.

autowds

Clear the configuration recovery defaults.

no autowds

【Parameter Description】-

【Default Configuration】 -

【Command Mode】 ap-config configuration mode / ap-group configuration mode

【Default Level】14

【Usage Guide】 Normal nonroot bridging does not require some features, but only when AP partners need access.

It can be configured in ap-config all, ap-config xxxx (single ap) mode, and ap-group mode. The priority relationship of the three is ap-config xxxx> ap-grop> ap-config all.

【Configuration Example】 The AC is configured with the automatic bridging function to open all the AP.

```
AC-FS(config-ap)# autowds
```

【Verification】 Use the show running-config and show ap-config running commands on the AC to view the autowds configuration information.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.2 bridge roam-threthold

Configure roaming parameter threshold under NONROOT (configurable in NONROOT mode).

bridge roam-threthold *num1 num2 num3 num4* [radio *radio-id*]

Clear the configuration recovery defaults.

no bridge roam-threthold [radio *radio-id*]

Clear the configuration recovery defaults.

default bridge roam-threthold [radio *radio-id*]

【Parameter Description】

Parameter	Description
num1	Start the roaming threshold, the default is 40
num2	The scan threshold begins with a default value of 15
num3	Roam switching threshold, with a default value of 5
num4	Roam switching time threshold, with a default value of 5
radio radio-id	Only the id of radio to options configured on AC

【Default Configuration】 Default opens

【Command Mode】 Interface configuration mode on the AP / The AP configuration mode on the AC

【Default Level】 14

【Usage Guide】 Fat AP generally does not require the user to configure these roaming parameters thresholds, only under a special environment, will require the threshold will be configured. NONROOT FIT is generally configured through pre-configuration on AP, not on AC, in addition, generally do not require users to configure these roaming parameters thresholds, only in special environments, the threshold will be configured.

This command requires professionals to recommend configuration values after the actual measurement and analysis of the application environment. Self-configuration of this command is not allowed, otherwise it will affect the roaming effect of WDS and even the use of WDS bridging.

If you need to configure NONROOT on the AC, you need professionals to fully understand the application environment and then modify the configuration. Be sure to make sure the configuration is correct, because once the modification is wrong, the NONROOT will lose connection with the AC.

The configuration modification parent command on the AC will take effect after committing.

【Configuration Example】 NONROOT roaming parameters are configured on AP: the roaming judgment starts when the current

connected ROOT signal strength is less than 45 (-50); add the ROOT when all ROOT signal strength is less than 15; roaming when the difference between the best ROOT and the current connected ROOT signal is greater than 5, and the last roaming time is greater than 3s.

```
AC-FS(config-if-Dot11radio 1/0)# station-role non-root-bridge
```

```
AC-FS(config-if-Dot11radio 1/0)# parent ssid AC-FS-root
AC-FS(config-if-Dot11radio 1/0)# bridge roam-threthold 45 15 5 3
```

2: Clear the NONROOT roaming parameter configuration on the AP:

```
AC-FS(config-if-Dot11radio 1/0)# no bridge roam-threthold
```

3: NONROOT roaming parameters are configured on AC: the roaming judgment starts when the current connected ROOT signal strength is less than 45 (-50); add the ROOT when all ROOT signal strength is less than 15; roaming when the difference between the best ROOT and the current connected ROOT signal is greater than 5, and the last roaming time is greater than 3s.

```
AC-FS(config-ap)# bridge roam-threthold 45 15 5 3 radio 2
AC-FS(config-ap)# wds config commit radio 2
```

【Verification】 1. Use the show running-config command on the AP to view the bridge roam-threthold configuration information.
2. Using the show ap-config wds-config command on the AC, you can view the bridge roam-threthold configuration information

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.3 bridge security

Configuring supports encryption bridging (configurable in NONROOT mode)

bridge security [radio *num*] { wpa | rsn } ciphers { aes } akm psk key { ascii | hex } *key*

【Parameter Description】

Parameter	Parameter
radio num	AC only configured only representing the configured RF port.
wpa	Configure the wpa authentication mode.

rsn	Configure the rsn authentication mode.
aes	Configure the aes encryption mode.
psk	Configure access authentication for pre-shared key authentication.
ascii	Specifies that the PSK password is a ASCII code.
hex	Specifies the PSK password as a hexadecimal character.
key	When choosing a password in the form of a ascii, the key represents the password in the form of a ASCII code, with a length limit to 8- -63 ASCII code characters. When choosing a password in the hex form, the key represents the password in the hexadecimal form, and the length must be 64 hexadecimal characters.

【Default Configuration】 -

【Command Mode】 The AP configuration mode on the AC

【Default Level】 14

【Usage Guide】 Only the NONROOT side requires a configuration. The NONROOT FAT is configurable directly, and the NONROOT FIT is configured on the AC.

It is necessary to ensure that the encrypted parameters are exactly the same as the encrypted network parameters to be accessed.

Under NONROOT, the bridge security command is configured on the AC, and it will take effect after committing.

【Configuration Example】 Configure NONROOT Encryption parameters on AC: After the encryption parameters are configured and successfully issued, NONROOT AP will start to scan. If there is a network with consistent encryption parameters nearby, it will be bridging.

```
AC-FS(config-ap)# bridge security radio 1 wpa ciphers aes akm psk key ascii 12345678
AC-FS(config-ap)# wds config commit radio 1
```

【Verification】 Use the show ap-config wds-config command on the AC to see if the bridge security has been configured

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.4 bridge vlan

Create the Delete vlan command under the Thin AP

bridge vlan vid

Clear the configuration

no bridge vlan vid

【Parameter Description】

Parameter	Description
vid	Create a vid of the deleted vlan.

【Default Configuration】 -

【Command Mode】 The AP configuration mode on the AC

【Default Level】 14

【Usage Guide】 Create the Delete vlan command on the AC

The command configures vlan information against the actual requirements and cannot create too much vlan to otherwise affect ap performance.

【Configuration Example】 1： Create vlan 2 / 3 / 5 (if the vlan does not exist on AP, it is created on AP)

```
AC-FS(config-ap)# bridge vlan 2
AC-FS(config-ap)# bridge vlan 3
AC-FS(config-ap)# bridge vlan 5
```

2: Delete vlan 5 (if the vlan to be deleted has no other creator, it is time to delete the vlan).

```
AC-FS(config-ap)# no bridge vlan 5
```

【Verification】 Use the show ap-config wds-config command on the AC to view the configuration information

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.5 bridge with-client

Configure whether support bridge coverage is enabled (work at WDS bridge only)

bridge with-client { enable | disable } [radio *radio-id*]

【Parameter Description】

Parameter	Description
enable	Support bridge coverage.
disable	Bridging coverage is not supported.
radio radio-id	Only the id of radio to options configured on AC.

【Default Configuration】 disable

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 If you need to support WDS, you must configure to enable bridge with-client.

⚠ Turning on the bridge cover function is not recommended.

⚠ Under NONROOT, the modified with-client command on AC requires commit before issuance is required.

【Configuration Example】 1: The radio 2 WDS bridge ROOT mode is configured on the AC to support bridge coverage.

```
AC-FS(config-ap)#bridge with-client enable radio 2
```

2: Radio 2 WDS bridging NONROOT mode is configured on AC.

```
AC-FS(config-ap)#bridge with-client enable radio 2
AC-FS(config-ap)#wds config commit radio 2
```

【Verification】 Use the show ap-config wds-config command on the AC to see if the bridge with-client has been enabled.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.6 parent

Configure ROOT information to connect in NONROOT mode (configurable in NONROOT mode)

parent { mac-address *HHHH.HHHH.HHHH* | ssid *ssid*} [radio *radio-id*]

Clear the configuration recovery defaults

no parent { mac-address | ssid } [radio *radio-id*]

【Parameter Description】

Parameter	Description
mac-address HHHH.HHHH.HHHH	Specify the BSSID of the ROOT terminal to access
ssid ssid	Specifying the SSID of the ROOT side to access will be in the eligible ROOT
radio radio-id	Only the id of radio to options configured on AC

【Default Configuration】 disable

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 The NONROOT end looking for the ROOT end through this command. If you need to use the WDS bridging function, the NONROOT side must configure parent related information. NONROOT FIT is generally configured by pre-configuration on AP, not on AC.

Fixed point-to-point bridging, it is recommended to use the parent mac-address configuration. If you need to enable the NONROOT roaming function, you need to use the parent ssid configuration.

If you need to configure NONROOT on the AC, you need professionals to fully understand the application environment and then modify the configuration. Be sure to make sure the configuration is correct, because once the modification is wrong, the NONROOT will lose connection with the AC.

The configuration modification parent command on the AC will take effect after committing.

【Configuration Example】 1: Modified configuration on the AC for NONROOT access to the ROOT terminal according to the BSSID.

```
AC-FS(config-ap)#no parent ssid radio 2
AC-FS(config-ap)#parent mac-address 00d0.f822.3301 radio 2 AC-
FS(config-ap)#wds config commit radio 2
```

2: Modified configuration on AC NONROOT access to the ROOT end according to SSID .

```
AC-FS(config-ap)#no parent mac-address radio 2
AC-FS(config-ap)#parent ssid AC-FS-root radio 2 AC-
FS(config-ap)#wds config commit radio 2
```

【Verification】 Use the show ap-config wds-config command on the AC to view the parent configuration information.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.7 show ap-config wds-bridge-info

View the WDS bridging information for the interface.

show ap-config wds-bridge-info { summary | *ap-name* radio *radio-id*}

【Parameter Description】

Parameter	Description
summary	Displays an AP list with a configured WDS.
ap-name	The name of the AP to query for the WDS bridging information.
radio-id	The id of the radio to query.

【Command Mode】 Privilege mode

【Default Level】 14

【Usage Guide】 Use this command to view the WDS bridging information for the ap

【Configuration Example】 1: View the WDS bridging information for the interface.

```
AC-FS#show ap-config wds-bridge-info summary
Ap Name       Mac Address     Radio  Station Role
------------  --------------  -----  ----------------

Ap-001        00d0.f822.3301  2      ROOT-BRIDGE
Ap-002        00d0.f822.3304  2      NONROOT-BRIDGE
```

2: View the WDS bridging information for the interface.

```
AC-FS# show ap-config wds-bridge-info Ap-001 radio 2 WDS-
MODE: ROOT-BRIDGE
BRIDGE-WLAN:
  Status OK
Wlanid 1, SSID AC-FS_root, BSSID 32d0.f822.3303

WBI 1/0
  NONROOT 00d0.f822.3304

WBI 1/1
   NONROOT 00d0.f822.3307
```

【Field interpretation】

Field	interpretation
WDS-MODE	WDS bridge pattern.
BRIDGE-WLAN	WLAN information used for bridging.
WBI	Established WDS, bridging link information.

3: View the WDS bridging information for the interface.

```
AC-FS# show ap-config wds-bridge-info Ap-002 radio 2 WDS-
MODE: NONROOT-BRIDGE
MAC：00d0.f822.3304

WBI 1/0
  ROOT 32d0.f822.3303
```

【Prompt Information】 -

【Platform Description】 -

1.8 show ap-config wds-config

View the WDS configuration information

show ap-config wds-config [*ap-name*]

【Parameter Description】

Parameter	Description
ap-name	The name of the AP to want to query the WDS configuration.

【Command Mode】 Privilege mode

【Default Level】 14

【Usage Guide】 Use this command to view the WDS bridging information for the ap

【Configuration Example】 1: View the WDS configuration information

```
AC-FS#show ap-config wds-config ap-
config 001a.1a03.027b
 station-role root-bridge bridge-wlan 1 radio 1
 station-role root-ap radio 2
 [Uncommit] station-role non-root-bridge radio 1
 bridge with-client enable radio 1
 bridge vlan 2
 bridge vlan 3
!
!!!!!
ap-config 00d0.f822.33b4
 station-role root-ap radio 1
```

2: View the WDS bridging information for the interface

```
AC-FS# show ap-config wds-config 001a.1a03.027b ap-
config 001a.1a03.027b
 station-role root-bridge bridge-wlan 1 radio 1
 station-role root-ap radio 2
 [Uncommit] station-role non-root-bridge radio 1
 bridge with-client enable radio 1
 bridge vlan 2
 bridge vlan 3
```

【Prompt Information】 -

【Platform Description】 -

1.9 station-role

Configure the bridging mode, and specify the corresponding parameters.

station-role { root-ap | root-bridge bridge-wlan *wlan-id*| non-root-bridge } [radio *radio-id*]

Clear the configuration recovery defaults

no station-role [radio *radio-id*]

【Parameter Description】

Parameter	Description
root-ap	The AP works in non-bridging mode, which is the default configuration.
root-bridge	AP works in WDS bridging ROOT mode.
non-root-bridge	AP works in WDS bridging NONROOT mode.
bridge-wlan wlan-id	Specifies the WLAN ID used for bridging in ROOT mode.
radio radio-id	Configure option on the AC, the id of the radio to configure.

【Default Configuration】 root-ap

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 If you need to use WDS bridging, you must configure the station-role to work in bridging mode. NONROOT FIT is generally configured by pre-configuration on AP, not on AC.

In the AP, in the WDS bridging ROOT mode, you must specify the WLAN ID of the WLAN for bridging. If the WLAN is not created, then The WDS bridge failed to start work. The WLAN can not be set to hide the SSID, otherwise NONROOT may not connect.

If a NONROOT-related configuration is required on the AC, professionals need to modify the configuration after having a full understanding of the application environment. Make sure to ensure correct configuration because NONROOT loses connection to the AC.

Under with-client in NONROOT mode, the number of WLAN the RF port can create depending on different product.

【Configuration Example】 1: The radio 2 configured with AP on the AC works in WDS bridging ROOT mode, and the WLAN for bridging is 1.

```
AC-FS(config-ap)# station-role root-bridge bridge-wlan 1 radio 2
```

2: The radio 1 for configuring AP on AC works in WDS bridging NONROOT mode (generally do not make a configuration modification nonroot on ac Related Configuration).

```
AC-FS(config-ap)# station-role non-root-bridge radio 1
```

```
AC-FS(config-ap)# parent mac-address 0001.0002.0003 radio 1
AC-FS(config-ap)# wds config commit radio 1
```

【Verification】 Use the show ap-config wds-config command on the AC to view the station-role configuration

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.10 wds config

No submission or clearing of valid command on AC after nonroot related command configuration

wds config [clear | commit] radio *radio-id*

【Parameter Description】

Parameter	Description
clear	Clear the inactive wds configuration.
commit	Submit an inactive wds configuration.
radio-id	The id of the radio s to configure.

【Default Configuration】 -

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 When configured with nonroot on AC or sync, wds edit mode is entered, where most wds configuration commands do not take effect immediately, requiring wds config commit.

After entering wds edit mode on AC, most of the wds configuration commands will not take effect immediately, and commit will be effective before being issued.

Since the nonroot configuration modifications need to be careful on the AC, make sure that the configuration is correct before performing the commit operation

After Wds config commit, the bridge will be disconnected and then reestablished.

【Configuration Example】1: Modify nonroot parent information on AC from parent ssid AC-FS-root to parent mac 0001.0002.0003 (not recommended to modify nonroot configuration on AC, complete configuration when pre-configuration on AP).

```
AC-FS(config-ap)# no parent ssid radio 2
AC-FS(config-ap)# parent mac-address 0001.0002.0003 radio 2 AC-
FS(config-ap)# wds config commit radio 2
```

2: Discards all inactive commands on the AC.For example, modify and discard the parent information in the above example：

```
AC-FS(config-ap)# no parent ssid radio 2
AC-FS(config-ap)# parent mac-address 0001.0002.0003 radio 2 AC-
FS(config-ap)# wds config clear radio 2
```

【Verification】 Using the show ap-config wds-config command, you can view the wds configuration information.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.11 wds ctrl eth

Configuration controls wired ports (configurable only when working in NONROOT mode).

wds ctrl eth

Clear the configuration.

no wds ctrl eth

【Parameter Description】 -

【Default Configuration】 Default closed

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 Only the NONROOT side requires a configuration. The NONROOT FAT is configurable directly, and the NONROOT FIT is configured on the AC

⚠ Care should be taken when configuring this command, because once the NONROOT is not bridging, the wired port will be

disconnected, and then the CAPWAP will be disconnected, resulting in the AC loses control of the AP.

【Configuration Example】 Configuration control wired ports on AC.

```
AC-FS(config-ap)#wds ctrl eth
```

【Verification】 Use the show ap-config running command on the AC to see if the wdsctrl eth is already enabled.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.12 wds head-chan

Configure front and rear channel (configurable in NONROOT mode).

wds head-chan *num1* tail-chan *num2* [radio *radio-id*]

Clear the configuration recovery defaults.

no wds head-chan [radio *radio-id*]

【Parameter Description】

Parameter	Description
num1	The front channel
num2	The front channel
radio radio-id	Only the id of radio to options configured on AC

【Default Configuration】 0

【Command Mode】 The AP configuration mode on the AC

【Default Level】 14

【Usage Guide】 Only the NONROOT side requires a configuration. The NONROOT FAT is configurable directly, and the NONROOT FIT is configured on the AC.



This command is that the NONROOT changes the channel value based on the current state (front or rear) for the purpose of switching channels.

Under NONROOT, the command is configured on AC before commit.

【Configuration Example】 Radio 2 WDS bridging NONROOT mode is configured on AC.

```
AC-FS(config-ap)# wds head-chan 36 tail-chan 52 radio 2
AC-FS(config-ap)#wds config commit radio 2
```

【Verification】 Using the show ap-config wds-config command on the AC, you can see if the wds head-chan has been configured.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.13 wds pre-config

The nonroot pre-configuration command, to delete the pre-configuration

wds pre-config [delete] [radio *radio-id*]

【Parameter Description】

Parameter	Description
delete	Remove the preconfiguration.
radio radio-id	Only the id of radio to options configured on AC.

【Default Configuration】 -

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 If working in the nonroot fit application scenario, the nonroot fit AP must be pre-configured first.

When the wds bridge working mode is not used, you need to use the wds pre-config delete command to delete the configuration file on the non-root side.

【Configuration Example】 Remove the radio 1 wds nonroot preconfiguration on the AC:

```
AC-FS(config-ap)# wds pre-config delete radio 1
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.14 wds security enable

Configure uring encryption (working on WDS bridge only)

wds security enable [radio *radio-id*]

Clear the configuration

no wds security enable [radio *radio-id*]

【Parameter Description】

Parameter	Description
radio radio-id	Only the id of radio to options configured on AC.

【Default Configuration】 Default closed.

【Command Mode】 The AP configuration mode on the AC.

【Default Level】 14

【Usage Guide】 If you need to use WDS to support the encryption capabilities, you must configure the enabling wds security enable.

This command is whether to encrypt the communication between NONROOT and ROOT; the configuration of encryption on both sides must be consistent, otherwise communication cannot be performed

Under NONROOT, the configuration modification wds security enable command on the AC will take effect after committing.

【Configuration Example】 1: The radio 2 WDS bridge ROOT mode is configured on the AC to support bridge coverage.

```
AC-FS(config-ap)#wds security enable radio 2
```

2: Radio 2 WDS bridging NONROOT mode is configured on AC.

```
AC-FS(config-ap)#wds security enable radio 2
AC-FS(config-ap)#wds config commit radio 2
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.15 wds-mode enable

Configure whether to switch to wds mode (support only ap use for bridging mode).

wds-mode enable

Clear the configuration.

Wds-mode disable

【Parameter Description】-

【Default Configuration】 Default closed

【Command Mode】 The AP configuration mode on the AC

【Default Level】 14

【Usage Guide】 -

【Configuration Example】 The radio 2 WDS bridge ROOT mode is configured on the AC to support bridge coverage.

```
AC-FS(config-ap)#wds-mode enable/disable
```

【Verification】 Using the show ap-config wds-mode summary command on the AC, you can view all of the ap wds mode capabilities.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.16 show ap-config wds-mode summary

Check on AC if online AP enables wds mode (only bridging mode).

show ap-config wds-mode summary

【Parameter Description】-

【Default Configuration】 Default closed

【Command Mode】 View by the show command on the AC

【Default Level】 14

【Usage Guide】 -

【Configuration Example】 Configure whether the WDS encryption feature on the AP.

```
show ap-config wds-mode summary
AP Name                    AP MAC        WDS MODE
_________________________________________________________________
```

【Verification】 Using the show ap-config wds-mode summary command on the AC allows the current online ap to see if the wds mode has been enabled.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

Chapter 6 Access Service

This volume introduces the relevant contents of the access service command manual, including the following chapters:

1. Interface
2. MAC address
3. VLAN
4. Super VLAN
5. MSTP
6. MAC VLAN
7. VLAN-Group
8. PPP
9. PPPOE-CLIENT
10. PPPOE-SERVER

1 Interface

1.1 bandwidth

Set the bandwidth parameter of the interface in interface configuration mode.

bandwidth kilobits

Restore the default value of Bandwidth Parameter.

no bandwidth

【Parameter Description】

Parameter	Description
kilobits	Bandwidth per second, in the unit of Kbps.

【Default Configuration】 When the bandwidth command Parameter is not set in the interface, use the show interface command in privileged user mode to display its default value.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 The bandwidth command cannot actually affect the bandwidth of an interface, but only allows the user to tell the system the bandwidth index of the interface. By default, the bandwidth of an Ethernet interface is determined according to the actual port link rate. Specify that Bandwidth is only a routing parameter, and does not affect the real bandwidth of the interface of the physical link.

【Configuration Example】 The following example sets the bandwidth on the interface to 64 Kbps.

```
AC-FS(config)#interface gigabitEthernet 0/1
AC-FS(config-if-GigabitEthernet 0/1)# bandwidth 64
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.2 carrier-delay

Use the command carrier-delay in the interface configuration mode to set the carrier delay on the interface.

carrier-delay [seconds]

Return the default value.

no carrier-delay

【Parameter Description】

Parameter	Description
seconds	Optional Parameter, in seconds, ranging from 0 to 60 seconds.

【Default Configuration】 The default value of carrier delay is 2 seconds.

【Command Mode】 Interface mode.

【Default Level】 14

【Usage Guide】 This parameter refers to the time delay of the carrier detection signal DCD of the interface link from the Down state to the Up state. If the DCD changes within the delay, the system will ignore the change of the state and will not cause The upper data link layer renegotiates.

If the DCD carrier is interrupted for a long time, set this parameter to be longer to speed up the route aggregation as soon as possible, so that the routing table can converge faster. If on the contrary, the DCD carrier interruption time is less than the time it takes for route aggregation, then this parameter should be set relatively large to avoid unnecessary route flapping.

【Configuration Example】 The following example sets the carrier delay of serial interface to 5 seconds.

```
AC-FS(config)# interface GigabitEthernet 1/1
AC-FS(config-if-GigabitEthernet 1/1)# carrier-delay 5
```

【Verification】1: Use the show interfaces command to view the carrier delay of the interface.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.3 clear counters

Use this command to clear the counters on the specified interface.

clear counters [interface-id]

【Parameter Description】

Parameter	Description
interface-id	Interface type and interface ID.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】The statistics of the interface can be viewed through the command show interfaces in privileged mode, and the statistics of the interface can be cleared by using the command clear counters in the privileged mode. If no interface is specified, all interface counters are cleared.

【Configuration Example】 The following example clears the counters on interface gigabitethernet 1/1.

```
AC-FS# clear counters GigabitEthernet 1/1
```

【Prompt Information】-

【Platform Description】-

1.4 clear interface

Use this command to reset the interface.

clear interface interface-id

【Parameter Description】

Parameter	Description

interface-id	Interface type and interface ID.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 This command is only valid for switch ports, member ports of Layer 2 aggregation ports, routing ports and member ports of Layer 3 aggregation ports. Executing this command is equivalent to executing the shutdown and no shutdown commands on the interface binding.

【Configuration Example】 The following example resets the interface gigabitethernet 1/1.

```
AC-FS# clear interface GigabitEthernet 1/1
```

【Prompt Information】-

【Platform Description】-

1.5 description

Set the alias for the interface.

description string

Restore to default value.

no description

【Parameter Description】

Parameter	Description
string	Interface alias.

【Default Configuration】 There is no alias by default.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 Use the show interfaces command to view interface information, including aliases.

【Configuration Example】 1: Configure the alias GBIC-1 for interface GigabitEthernet 1/1.

```
AC-FS(config)# interface GigabitEthernet 1/1
AC-FS(config-if-GigabitEthernet 1/1)# description GBIC-1
```

【Verification】1: Use the show interfaces command to view the alias of the interface.

2: Use the show interfaces description command to view the aliases of the interfaces.

【Prompt Information】 1: If the alias length exceeds 80, it will prompt an error.

```
% The length of description is up to 80!
```

【Common Mistake】-

【Platform Description】-

1.6 duplex

Sets the duplex mode of the interface.

duplex { auto | full | half }

Restore to default value.

no duplex

【Parameter Description】

Parameter	Description
auto	Self-adaptive full duplex and half duplex.
full	Full duplex.
half	Half duplex.

【Default Configuration】 Full-duplex and half-duplex self-adaptation.

【Command Mode】 Interface mode

【Default Level】 14

【Usage Guide】The duplex attribute of an interface is related to the type of the interface. The interface duplex settings can be viewed

with the show interfaces command.

【Configuration Example】 1: Configure the duplex mode of interface GigabitEthernet 1/1 to full duplex.

```
AC-FS(config)# interface GigabitEthernet 1/1
AC-FS(config-if-GigabitEthernet 1/1)# duplex full
```

【Verification】1: Use the show interfaces command to view the duplex mode of the interface.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.7 errdisable recovery

Set port violation recovery.

errdisable recovery [interval time]

【Parameter Description】

Parameter	Description
interval time	Optional configuration, set the automatic recovery interval, if not selected, it means manual recovery, no automatic recovery function, the value range is 30-86400, the unit is seconds.

【Default Configuration】 Default port violation will not be recovered.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】When a violation occurs, use show interfaces status err-disable to view the cause of the violation, and use this command to restore the port after troubleshooting the network fault.

【Configuration Example]】1: Recover the violating port from the error state.

```
AC-FS(config)# errdisable recovery
AC-FS(config)# end
```

【Verification】1: Use the show interfaces status err-disable command to view the port violation information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.8 interface

Use this command to enter the interface configuration mode.

interface interface-typeinterface-number

【Parameter Description】

Parameter	Description
interface-type	The interface type.
interface-number	The interface ID.

【Default Configuration】-

【Command Mode】 Interface mode

【Default Level】 14

【Usage Guide】 This command enters the interface configuration mode, and the next step is to modify the interface configuration.

【Configuration Example】 1. The following example enters configuration mode on Aggregateport 1.

```
AC-FS(config)# interface Aggregateport 1
AC-FS(config-if-Aggregateport 1)#
```

2. The following example enters configuration mode on GigabitEthernet 1/2.

```
AC-FS(config)# interface GigabitEthernet 1/2
AC-FS(config-if-GigabitEthernet 1/2)#
```

3. The following example configuration mode on VLAN 1.

```
AC-FS(config)# interface vlan 1
AC-FS(config-if-VLAN 1)#
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.9 interface range

Use the interface command in global configuration mode to enter interface configuration mode.

Interface range { port-range | macro macro_name }

The macro names in the above command are defined using define interface-range.

define interface-range macro_name

【Parameter Description】

Parameter	Description
port-range	The interface type and ID range, entered in the form of interface-type slot-number/interface-number. The interface can be either an Ethernet physical interface or a loopback interface.
macro macro_name	The macro name which represents the interface range.

【Default Configuration】 By default, this function is not used.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】When using macro definition, you need to define a certain range of interface types as macro_name through the define

interface-range command in the global configuration mode, and then use the interface range macro macro_name to perform interface batch configuration management.

【Configuration Example】 1. The following example enters interface configuration mode on multiple interfaces by setting the interface.

```
AC-FS(config)# interface range gigabitEthernet 0/0, 0/2
AC-FS(config-if-range)# bandwidth 100
```

2: Enter the macro name to configure the interface configuration in batches.

```
AC-FS(config)# define interface-range route1 gigabitEthernet 0/0-2 AC-
FS(config)# interface range macro route1
AC-FS(config-if-range)# bandwidth 100
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.10 load-interval

Specifies the interval for load calculation of an interface in interface configuration mode.

load-interval seconds

Restore Default Configuration.

no load-interval

【Parameter Description】

Parameter	Description
seconds	In the range from 5 to 600 in the unit of seconds.

【Default Configuration】10 seconds.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 1: Use this command on an interface to specify how often to calculate the input and output load of packets, generally every 10 seconds to calculate the number of input and output packets and bits per second. For example, if you change this parameter to 180 seconds in interface GigabitEthernet 0/1, you can see it with show interface gigabitEthernet 0/1:

```
3 minutes input rate 15 bits/sec, 0 packets/sec
3 minutes output rate 14 bits/sec, 0 packets/sec
```

【Configuration Example】 1: The following example demonstrates how to set the load calculation interval to 180 seconds in the Ethernet port GigabitEthernet 0/1.

```
AC-FS(config)# interface gigabitEthernet 0/1
AC-FS(config-if-GigabitEthernet 0/1)# load-interval 180
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.11 logging

Configure information about the print interface.

logging [link-updown | error-frame | link-dither]

【Parameter Description】

Parameter	Description
link-updown	Prints the status change information.
error-frame	Prints the error frame information.
link-dither	Prints the oscillation information.

【Default Configuration】 This function is enabled.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 It is up to the user to decide whether to open the printing interface related information. It is enabled by default. When the interface status changes, the interface receives an error frame or the interface flaps, the information when the interface discards the received frame due to insufficient resources, and the Prompt Information when the interface receives a CRC error packet, print Prompt Information. After configuring no logging [link-updown | error-frame | link-dither], Prompt Information will not be printed.

【Configuration Example】 1: Configure the status change information of the print interface.

```
AC-FS(config)# logging link-updown
AC-FS(config)# logging error-frame
AC-FS(config)# logging link-dither
```

【Verification】-

【Prompt Information】 -Prompt Information when the interface state changes:

%LINK-3-UPDOWN: Interface GigabitEthernet 0/0, changed state to up.

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/0, changed state to up.

Prompt Information when the interface receives an error frame:

%PORT-3-ERR_FRAME: Received error frames on interface GigabitEthernet 0/0. Please check the physical link.

Prompt Information when the interface flaps:

%LINK-4-DITHER: The state of Interface GigabitEthernet 0/1 is astable. Please check the physical link.

%LINK-4-DITHER: The state of interface GigabitEthernet 0/1 is astable and the interface will be shutdown. Please check the physical link

【Common Mistake】-

【Platform Description】-

1.12 medium-type

Select the media type for the interface.

medium-type { auto-select [prefer [fiber | copper]] | fiber | copper }

Restore to default value.

no medium-type

【Parameter Description】

Parameter	Description
fiber	Optical interface.
prefer [fiber | copper]	The preferred medium type for the interface is selected.
auto-select	Auto-selects the medium type for the interface.
copper	Copper interface.

【Default Configuration】 The default is the electrical port.

【Command Mode】 Interface configuration mode (physical port)

【Default Level】 14

【Usage Guide】 If the same port can choose two media types, optical port and electrical port, the user can only use one of them. Once the media type is determined, when configuring the properties of the port, such as status, duplex, flow control, and speed, all refer to the properties of the currently selected type of the port. After changing the port type, the properties of the port corresponding to the new type are the default properties, which can be reconfigured by the user as required.

If the user configures the port media to be automatically selected, when only one medium is connected to the port, the device uses the currently connected medium; when both media are connected to the port, the device will use the user-configured preferred medium. The medium auto-select preferred medium is the electrical port by default, and the user can set the medium-type auto-select prefer fiber to the optical port by configuring the medium-type auto-select prefer fiber. In automatic selection mode, the port's speed, duplex, flow control and other attributes will use the default values.

【Configuration Example】1: Port GigabitEthernet 1/1 is an optical port, set the medium type to an electrical port.

```
AC-FS(config)# interface GigabitEthernet 1/1
AC-FS(config-if-GigabitEthernet 1/1)# medium-type copper
```

【Verification】1: Use the show interfaces command to view the media type of the interface.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.13 mtu

Set the MTU of the interface

mtu num

【Parameter Description】

Parameter	Description
num	64—? (The maximum value is different for different products, determined by the chip)

【Default Configuration】 The default value is 1500.

【Command Mode】 Interface mode

【Default Level】 14

【Usage Guide】 Set the MTU supported by the interface, that is, the maximum length of the data part of the link layer. Currently only supports setting the MTU of the physical port.

【Configuration Example】1: Set the MTU of port GigabitEthernet 1/1 to 9000.

```
AC-FS(config)# interface GigabitEthernet 1/1
AC-FS(config-if-GigabitEthernet)# mtu 9000
```

【Verification】1: Use the show interfaces command to view the MTU of the interface.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.14 physical-port dither protect

Configure interface flapping protection.

physical-port dither protect

【Parameter Description】-

【Default Configuration】 This function is enabled.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 The port link flapping protection function is up to the user to decide whether to enable it. By default, the protection function is enabled, that is, physical-port dither protect. When the interface flaps and exceeds a certain number of times, the port will be shut down to protect the port. After configuring the no physical-port dither protect command, only print Prompt Information, do not close the interface.

Description:

The interface detects flapping every 2s or 10s. If it detects that the interface flaps 6 times in 2s, and prints the Prompt Information, and prints the Prompt Information continuously for 10 times (that is, the interface flaps are detected continuously within 20s), the interface is shut down. For 10s detection of one vibration, if the number of vibrations exceeds 10 times, Prompt Information will be printed, and the interface will not be closed.

【Configuration Example】1: Enable the flapping protection function of the interface.

```
AC-FS(config)# physical-port dither protect
```

【Verification】-

【Prompt Information】-Prompt Information when the interface sends flapping:

If the interface detects 6 flaps within 2s or 10 flaps within 10s, the following information is displayed:

%LINK-4-DITHER: The state of Interface GigabitEthernet 0/1 is astable. Please check the physical link.

The interface sends 10 oscillations within 20s, and the last oscillation prompt information is:

%LINK-4-DITHER: The state of interface GigabitEthernet 0/1 is astable and the interface will be put in err-disable state. lease check the physical link.

【Common Mistake】-

【Platform Description】-

1.15 shutdown

In interface configuration mode, use this command to shut down an interface.

shutdown

Open the interface.

no shutdown

【Parameter Description】

【Default Configuration】 The management state of the interface is UP.

【Command Mode】 Interface mode

【Default Level】 14

【Usage Guide】 For an interface (Ethernet port, aggregated port and switched virtual interface), this command closes the interface, and other configurations of the interface still exist, but have no effect. Use the show interfaces command to view interface status.

【Configuration Example】 1: Turn off aggregate port 1.

```
AC-FS(config)# interface Aggregateport 1
AC-FS(config-if-Aggregateport 1)# shutdown
```

2: Open aggregate port 1.

```
AC-FS(config)# interface Aggregateport 1
AC-FS(config-if-Aggregateport 1)# no shutdown
```

【Verification】 1: Use the show interfaces switchport command to view the Layer 2 information of the port.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.16 snmp trap link-status

In the device, you can configure whether to send the LinkTrap of the interface based on the interface configuration. When the function is

enabled, if the Link state of the interface changes, SNMP will send the LinkTrap, otherwise it will not send it.

snmp trap link-status

Disable this function, SNMP will not send LinkTrap.

no snmp trap link-status

【Parameter Description】-

【Default Configuration】 By default, this function is enabled.

【Command Mode】 Interface mode.

【Default Level】 14

【Usage Guide】 For an interface (Ethernet port, aggregated port and switched virtual interface), this command configures whether to send the LinkTrap of the interface. When the function is enabled, if the Link state of the interface changes, SNMP will send the LinkTrap, otherwise it will not send the LinkTrap. .

【Configuration Example】 1: The following example configures the interface not to send LinkTrap.

```
AC-FS(config)# interface GigabitEthernet 1/1
AC-FS(config-if-GigabitEthernet 1/1)# no snmp trap link-status
```

2: The following example configures the interface to send LinkTrap.

```
AC-FS(config)# interface GigabitEthernet 1/1
AC-FS(config-if-GigabitEthernet 1/1)# snmp trap link-status
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.17 snmp-server if-index persist

Enable the interface index persistence function, that is, the interface index does not change after the device restarts.

snmp-server if-index persist

【Parameter Description】-

【Default Configuration】 This function is disabled.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 After executing the command "snmp-server if-index persist", the indexes of all current interfaces will be saved when the configuration is saved, and the interface will use the interface index assigned before the restart after restarting. Note that the configuration must be guaranteed before restarting.

【Configuration Example】 1: Enable the interface index permanent function.

```
AC-FS(config)# snmp-server if-index persist
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.18 speed

Set the speed of the interface.

speed [10 | 100 | 1000 | auto]

Restore to default value.

no speed

【Parameter Description】

Parameter	Description
10	Indicates that the rate of the interface is 10Mbps.

100	Indicates that the rate of the interface is 100Mbps.
1000	Indicates that the rate of the interface is 1000Mbps.
auto	Indicates that the rate of the interface is adaptive.

【Default Configuration】 The default rate is adaptive.

【Command Mode】 Interface mode

【Default Level】 14

【Usage Guide】If an interface is a member of an aggregate port, the rate of the interface is determined by the rate of the aggregate port. The interface uses its own rate setting when it exits the aggregated port. Use the show interfaces command to view the settings. Different interface types will allow different rate types to be set. For example, SFP type interfaces are not allowed to set the rate to 10M.

【Configuration Example】 1: Set the rate of port GigabitEthernet 1/1 to 100Mbps.

```
AC-FS(config)# interface GigabitEthernet 1/1
AC-FS(config-if-GigabitEthernet 1/1)# speed 100
```

【Verification】 1: Use the show interfaces command to view the interface rate.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.19 1.18 switchport

Use the switchport command without any Parameter in interface configuration mode to set an interface to Layer 2 mode.

switchport

Use the no switchport command without any Parameter to set the interface to Layer 3 mode.

no switchport

【Parameter Description】

【Default Configuration】 By default, all interfaces are in Layer 2 mode.

【Command Mode】 Interface mode

【Default Level】 14

【Usage Guide】This command is only valid for the interface associated with the physical port. The operation of the switchport command will close the interface and reopen it, during which time the device will issue a message indicating the status of the connection. If you switch an interface from Layer 2 mode to Layer 3 mode, all Layer 2 properties for that interface are removed.

【Configuration Example】 1: Set port GigabitEthernet 0/1 to Layer 2 mode.

```
AC-FS(config)# interface GigabitEthernet 0/1
AC-FS(config-if-GigabitEthernet 0/1)# switchport
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.20 switchport access

Make a port an Access port and assign it as a member port of a VLAN.

switchport access vlan vlan-id

Assign the port to the default VLAN.

no switchport access vlan

【Parameter Description】

Parameter	Description
vlan-id	The ID of the VLAN to which the port is to be added.

【Default Configuration】 The default mode of the port is Access, and the default VLAN is VLAN 1.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 Enter a VLAN ID. If a new VLAN ID is entered, the device creates a VLAN and sets the port as a member of that VLAN. If you enter an existing VLAN ID, add a member port of the VLAN. If the port is a trunkport, this operation will have no effect.

【Configuration Example】 1: Set port GigabitEthernet 1/1 as a member port of VLAN 2.

```
AC-FS(config)# interface GigabitEthernet 1/1
AC-FS(config-if-GigabitEthernet 1/1)# switchport access vlan 2
```

【Verification】 1: Use the show interfaces switchport command to view the Layer 2 information of the port.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.21 switchport mode

Specifies the mode of a Layer 2 port, which can be specified as an Access port or a Trunk port.

switchport mode {access | trunk}

Restore the mode of the interface to the default value.

no switchport mode

【Parameter Description】

Parameter	Description
access	Set the Layer 2 port as the Access port.
trunk	Set the Layer 2 port as a Ttrunk port.

【Default Configuration】 The default mode of the Layer 2 port is Access.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 If the port mode is Access, the port can only be a member of one VLAN. You can use the switchport access vlan command to specify which VLAN the interface is a member of.

If the mode of a port is trunk, the interface can be a member of multiple VLANs. Which VLANs the interface can belong to is determined by the interface's permitted VLAN list, and the trunk port is a member of all VLANs in the permitted VLAN list. You can use the switchport trunk command to define a list of permitted VLANs for an interface.

【Default Configuration】 1: Configure port GigabitEthernet 1/1 as a trunk port.

```
AC-FS(config)# interface GigabitEthernet 1/1
AC-FS(config-if-GigabitEthernet 1/1)# switchport mode trunk
```

【Verification】 1: Use the show interfaces switchport command to view the Layer 2 information of the port.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.22 switchport trunk

Specify a native VLAN for a trunk port and configure a list of allowed VLANs.

switchport trunk { allowed vlan { all | [add | remove | except] vlan-list } | native vlan vlan-id }

Restore the trunk attribute of the interface to its default value.

no switchport trunk { allowed vlan | native vlan }

【Parameter Description】

Parameter	Description
allowed vlan vlan-list	Configure the list of permitted VLANs for the trunk port. Parameter vlan-list can be a VLAN or a series of VLANs, starting with a small VLAN ID and ending with a large VLAN ID. (-) Symbolic link. Such as: 10-20. Segments can be separated by (,) symbols, such as: 1-10, 20-25, 30, 33 all means that the list of permitted VLANs includes all supported VLANs; add means to add the specified VLAN list to the allowed VLAN list;

	remove means to remove the specified VLAN list from the permitted VLAN list; except means to add all VLANs except the listed VLAN list to the allowed VLAN list;
native vlan vlan-id	Configure Native VLAN.

【Default Configuration】 The default allowed VLAN list setting is all, and the default Native VLAN is VLAN 1.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 1. Native VLAN:

As a trunk port, it must belong to a native VLAN. The so-called native VLAN means that the UNTAG packets sent and received on this interface are considered to belong to this VLAN. Obviously, the default VLAN ID of this interface (that is, the PVID in IEEE 802.1Q) is the VLAN ID of the native VLAN. At the same time, when sending frames belonging to native VLAN on the Trunk port, UNTAG must be adopted.

2. Permitted VLAN list:

By default, a trunk port can transmit the traffic of all VLANs (1-4094) supported by the device. However, it is also possible to restrict the traffic of certain VLANs from passing through this Trunk port by setting the allowed VLAN list of the Trunk port.

【Configuration Example]】1: Configure the Native VLAN of GigabitEthernet 1/1 on the trunk port as VLAN 2.

```
AC-FS(config)# interface GigabitEthernet 1/1
AC-FS(config-if-GigabitEthernet 1/1)# switchport trunk native vlan 2
```

【Verification】1: Use the show interfaces switchport command to view the Layer 2 information of the port.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.23 show interfaces

View interface setting information.

show interfaces [interface-type interface-number] [description | switchport | trunk]

【Parameter Description】

Parameter	Description
interface-type interface-number	Interface type and interface number.
description	Description of the interface, including link status.
switchport	Layer 2 interface information, valid only for Layer 2 interfaces.
trunk	Trunk port information, valid for physical ports and aggregated ports.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 If no Parameter is added, the basic information of the interface will be displayed.

【Configuration Example]】1: When GigabitEthernet 0/1 is the trunk port, check the interface information.

```
SwitchA#show interfaces GigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN  , line protocol is DOWN
  Hardware is Broadcom 5464 GigabitEthernet, address is 00d0.f865.de9b (bia 00d0.f865.de9b)
  Interface address is: no ip address
  Interface IPv6 address is:
    No IPv6 address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Ethernet attributes:
    Last link state change time: 2012-12-22 14:00:48
    Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds
    Priority is 0
    Medium-type is Copper
    Admin duplex mode is AUTO, oper duplex is Unknown
    Admin speed is AUTO, oper speed is Unknown
    Flow receive control admin status is OFF,flow send control admin status is OFF
    Flow receive control oper status is Unknown,flow send control oper status is Unknown
    Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
  Bridge attributes:
    Port-type: trunk
    Native vlan:1
    Allowed vlan lists:1-4094                //List of allowed VLANs on the Trunk port
    Active vlan lists:1, 3-4 The actual vlans in effect (i.e. only VLANs 1, 3
and 4 are created on the device)
  Queueing strategy: FIFO
    Output queue 0/0, 0 drops;
    Input queue 0/75, 0 drops
  Rxload is 1/255,Txload is 1/255
  5 minutes input rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    0 packets output, 0 bytes, 0 underruns , 0 dropped
    0 output errors, 0 collisions, 0 interface resets
```

2: When GigabitEthernet 0/1 is the Access port, check the interface information.

```
SwitchA#show interfaces GigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN  , line protocol is DOWN
  Hardware is Broadcom 5464 GigabitEthernet, address is 00d0.f865.de9b (bia 00d0.f865.de9b)
  Interface address is: no ip address
  Interface IPv6 address is:
    No IPv6 address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Ethernet attributes:
    Last link state change time: 2012-12-22 14:00:48
    Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds
    Lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
    Priority is 0
    Medium-type is Copper
    Admin duplex mode is AUTO, oper duplex is Unknown
    Admin speed is AUTO, oper speed is Unknown
    Flow receive control admin status is OFF,flow send control admin status is OFF
    Flow receive control oper status is Unknown,flow send control oper status is Unknown
    Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
  Bridge attributes:
    Port-type: access
    Vlan id : 2                          //The VLAN ID of the Access port
  Queueing strategy: FIFO
    Output queue 0/0, 0 drops;
    Input queue 0/75, 0 drops
  Rxload is 1/255, Txload is 1/255
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
```

```
    0 packets output, 0 bytes, 0 underruns , 0 dropped
    0 output errors, 0 collisions, 0 interface resets
```

3: When GigabitEthernet 0/1 is a Hybrid port, check the interface layer 2 information.

```
SwitchA#show interfaces GigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN  , line protocol is DOWN
  Hardware is Broadcom 5464 GigabitEthernet
  Interface address is: no ip address
  Interface IPv6 address is:
    No IPv6 address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Ethernet attributes:
    Last link state change time: 2012-12-22 14:00:48
    Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds
    Lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
    Priority is 0
    Medium-type is Copper
    Admin duplex mode is AUTO, oper duplex is Unknown
    Admin speed is AUTO, oper speed is Unknown
    Flow receive control admin status is OFF,flow send control admin status is OFF
    Flow receive control oper status is Unknown,flow send control oper status is Unknown
    Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
  Bridge attributes:
    Port-type: hybrid
    Tagged vlan id:2                          // marked VLAN ID
    Untagged vlan id:none                    //Untagged VLAN ID
  Queueing strategy: FIFO
    Output queue 0/0, 0 drops;
    Input queue 0/75, 0 drops
  Rxload is 1/255 ,Txload is 1/255
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    0 packets output, 0 bytes, 0 underruns , 0 dropped
    0 output errors, 0 collisions, 0 interface resets
```

4: View the Layer 2 information of GigabitEthernet 0/1.

```
AC-FS# show interfaces GigabitEthernet 0/1 switchport
Interface               Switchport Mode      Access Native Protected VLAN lists
----------------------- ---------- --------- ------ ------ --------- ----------
GigabitEthernet 0/1     enabled    ACCESS    2      1      Disabled  ALL
```

【Prompt Information】-

【Platform Description】-

1.24 show interfaces counters

View statistics on the sending and receiving of packets on an interface.

show interfaces [interface-type interface-number] counters [increment | error | rate | summary]

【Parameter Description】

Parameter	Description
interface-type interface-number	Optional Parameter, interface type and interface number, if not selected, all interfaces will be displayed
increment	View the statistics of packets increased in the last sampling interval
error	View error message statistics.
rate	Check the rate of sending and receiving packets on the interface.
summary	View brief statistics on interface packets.

【Command Mode】 All CLI user modes

【Default Level】 14

【Usage Guide】 If no interface name is specified, the packet statistics of all interfaces will be displayed.

【Configuration Example]】1: Display the interface statistics of interface GigabitEthernet 0/1.

```
AC-FS#show interfaces GigabitEthernet 0/1 counters
Interface : GigabitEthernet 0/1
5 minute input rate  : 9144 bits/sec, 9 packets/sec
5 minute output rate : 1280 bits/sec, 1 packets/sec
Rxload               : 1%
InOctets             : 17310045
InPkts               : 1000(Unicast: 10%, Multicast: 10%, Broadcast: 80%)
InUcastPkts          : 100
InMulticastPkts : 100
InBroadcastPkts      : 800
Txload               : 1%
```

```
OutOctets            : 1282535
OutPkts              : 1000(Unicast: 10%, Multicast: 10%, Broadcast: 80%)
OutUcastPkts         : 100
OutMulticastPkts     : 100
OutBroadcastPkts     : 800
Undersize packets : 0
Oversize packets     : 0
collisions           : 0
Fragments            : 0
Jabbers              : 0
CRC alignment errors : 0
AlignmentErrors      : 0
FCSErrors            : 0
dropped packet events (due to lack of resources): 0
packets received of length (in octets):
  64:46264
  65-127: 47427
  128-255: 3478
  256-511: 658
  512-1023: 18016
  1024-1518: 125
Packet increment in last sampling interval(5 seconds):
  InOctets             : 10000
  InPkts               : 1000(Unicast: 10%, Multicast: 10%, Broadcast: 80%)
  InUcastPkts          : 100
  InMulticastPkts      : 100
  InBroadcastPkts      : 800
  OutOctets            : 10000
  OutPkts              : 1000(Unicast: 10%, Multicast: 10%, Broadcast: 80%)
  OutUcastPkts         : 100
  OutMulticastPkts     : 100
```

Description:

Rxload is the receive bandwidth utilization, and Txload is the transmit bandwidth utilization. InPkts is the sum of unicast, multicast and broadcast received, and the percentage of unicast, multicast and broadcast in parentheses. OutPkts are similar.

Packet increment in last sampling interval(5 seconds) is the packet increment statistics value of the last sampling interval (5 seconds).

2: Display the statistics of the packets added by interface GigabitEthernet 0/1 in the last sampling interval.

```
AC-FS#show interfaces GigabitEthernet 0/1 counters increment
Interface : GigabitEthernet 0/1
Packet increment in last sampling interval(5 seconds):
```

3: Display the statistics of error packets on interface GigabitEthernet 0/1.

```
  InOctets              : 10000
  InPkts                : 1000(Unicast: 10%, Multicast: 10%, Broadcast: 80%)
  InUcastPkts           : 100
  InMulticastPkts       : 100
  InBroadcastPkts       : 800
  OutOctets             : 10000
  OutPkts               : 1000(Unicast: 10%, Multicast: 10%, Broadcast: 80%)
  OutUcastPkts          : 100
  OutMulticastPkts      : 100
```

```
AC-FS#show interfaces GigabitEthernet 0/1 counters increment
Interface    UnderSize           OverSize            Collisions          Fragments

Gi0/1        0                   0                   0                   0
Interface    Jabbers             CRC-Align-Err       Align-Err           FCS-Err

Gi0/1        0                   0                   0                   0
```

Description:

UnderSize is the number of well-formed packets less than 64 bytes in length; OverSize is the number of well-formed packets greater than 1518 bytes in length. Collisions is the number of packets that collided when sent;
Fragments is the number of packets with CRC errors or alignment errors less than 64 bytes;
Jabbers is the number of packets with CRC errors or alignment errors greater than 1518 bytes;
CRC-Align-Err is the number of packets received with CRC errors number of messages;
Align_Err is the number of received packets with frame alignment errors; FCS-Err is the number of received packets with FCS errors.

4. Display the packet sending and receiving rate information on the interface GigabitEthernet 0/1 AC-FS#show interface gigabitEthernet 0/1 counters rate

```
Interface    Sampling Time       Input Rate          Input Rate          Output    Rate
Output Rate
                                 (bits/sec)          (packets/sec)       (bits/sec)
(packets/sec)

-------------------------------------------------------------------------------------

Gi0/1        5 seconds           23391               23                  124
0
```

Description:

```
Sampling Time is the sampling time of interface packets,
Input Rate is the rate at which interface packets are
received, and Output Rate is the rate at which interface
packets are sent.

5. Display brief statistics of packets on interface
GigabitEthernet 0/1 AC-FS#show
interface gigabitEthernet 0/1 counters summary
```

Interface	InOctets	InUcastPkts	InMulticastPkts	InBroadcastPkts
Gi0/1	1475788005	1389	45880503	11886621
Interface	OutOctets	OutUcastPkts	OutMulticastPkts	OutBroadcastPkts
Gi0/1	6667915	6382	31629	13410

Description:

InOctets is the total number of bytes of packets received by the interface, InUcastPkts is the number of unicast packets received by the interface, InMulticastPkts is the number of multicast packets received by the interface, and InBroadcastPkts is the number of broadcast packets received by the interface;

OutOctets is the total number of bytes sent by the interface, OutUcastPkts is the number of unicast packets sent by the interface, OutMulticastPkts is the number of multicast packets sent by the interface, and OutBroadcastPkts is the number of broadcast packets sent by the interface.

【Prompt Information】-

【Platform Description】-

1.25 show interfaces ethernet brief

View Ethernet information on an interface。

show interfaces [interface-type interface-number] ethernet brief

【Parameter Description】

Parameter	Description
interface-type interface-number	Optional Parameter, interface type and interface number, if not selected, all interfaces will be displayed.

【Command Mode】 All CLI user modes

【Default Level】 14

【Usage Guide】 If you do not specify an interface name, the Ethernet information of all interfaces will be displayed, including the link status information of the interface, the VLAN to which it belongs, auto-negotiation mode, duplex mode, interface speed, bandwidth utilization, and Description information (alias).

The supported interface types include physical ports, aggregated ports, and management ports.

【Configuration Example】1: Display the interface brief information of interface GigabitEthernet 0/1.

```
AC-FS#show interfaces GigabitEthernet 0/1 ethernet brief
down: link down
```

```
*down: administratively down
disabled: err-disabled(Please reference to command [show interface status err-disabled] for detail.)
Interface  Link Stat  Vlan  Auto-Neg  Duplex  Speed  Input Usage  Output Usage  Description
---------  ---------  ----  --------  ------  -----  -----------  ------------  -----------
Gi0/1        down       1     OFF       Unknown  Unknown  0.00%.....0.00%          10G port
```

Description:

Link Stat is the link status of the interface. If it is in the disabled state, you can use the show interface status err-disabled command to query the reason for the violation of the interface. If it is in the *down state, it means that the shutdown command is configured on the interface.

Vlan is the VLAN to which the interface belongs;

Auto-Neg is the auto-negotiation mode, ON means to enable auto-negotiation, when the port does not support the configuration of the auto-negotiation mode, it is displayed as --; Duplex is the duplex mode, and the valid value is displayed only when the interface link status is UP;

Speed is the interface speed, and the valid value will be displayed only when the interface link status is UP;

Input Usage is the bandwidth utilization of the interface receiving, and Output Usage is the bandwidth utilization of the interface. If the bandwidth utilization is less than 0.01% and there is traffic, it will display 0.01%, and the management port does not support bandwidth utilization, and it will be displayed as --;

Description is the description information (alias) of the interface, which is configured through the command description string.

【Prompt Information】-

【Platform Description】-

1.26 show interfaces link-state-change statistics

Check the time and number of port link status changes.

show interfaces [interface-type interface-number] link-state-change statistics

【Parameter Description】

Parameter	Description
interface-type interface-number	Interface type and interface number.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 If no interface name is specified, the link state change information of all interfaces will be displayed.

【Configuration Example】1: Display the link status change information of interface GigabitEthernet 0/1.

```
AC-FS# show interfaces GigabitEthernet 0/1 link-state-change statistics
Interface     Link state     Link state change times      Last change time
------------  ---------      -----------------------      --------------------

Gi 0/1        down           100                          2012-12-24 15:00:00
```

Interface	interface information.
Link state	current link status.
Link state change times	Link state changes.
Last change time	Time of the last link state change.

【Prompt Information】-

【Platform Description】-

1.27 show interfaces status

View the status information of the interface.

show interfaces [interface-type interface-number] status

【Parameter Description】

Parameter	Description
interface-type interface-number	Interface type and interface number.
status	View various status information of the interface, including speed and duplex.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 If no interface name is specified, the status information of all interfaces will be displayed.

【Configuration Example】1: Display the status information of interface GigabitEthernet 0/1.

```
AC-FS#show interfaces GigabitEthernet 0/1 status
Interface               Status       Vlan     Duplex  Speed   Type
──────────────────────  ──────────   ──────   ──────  ──────  ──────
GigabitEthernet 0/1     up           1        Full    1000M   copper
```

【Prompt Information】-

【Platform Description】-

1.28 show interfaces status err-disable

View status information for interface violations.

show interfaces [interface-type interface-number] status err-disable

【Parameter Description】

Parameter	Description
interface-type interface-number	Optional Parameter, interface type and interface number, if not selected, all interfaces will be displayed.

【Command Mode】 All CLI user modes

【Default Level】 14

【Usage Guide】 If no interface name is specified, the port violation status information of all interfaces will be displayed.

【Configuration Example]】1: Display the port violation status information of interface GigabitEthernet 0/1.

```
AC-FS#show interface gigabitEthernet 0/1 status err-disabled
Interface                      Status          Reason
------------------------------ --------------- ----------------

GigabitEthernet 0/1            err-disabled    BPDU Guard
```

Description: Status is whether the port violates or not. It displays err-disable if there is a violation. If there is no violation, it will not display it. Reason indicates the reason for the violation. If there is no violation, it will not be displayed.

【Prompt Information】-

【Platform Description】-

1.29 show interfaces usage

View interface bandwidth utilization.

show interfaces [interface-type interface-number] usage

【Parameter Description】

Parameter	Description
interface-type interface-number	Optional Parameter, interface type and interface number, if not selected, all interfaces will be displayed.

【Command Mode】 All CLI user modes

【Default Level】 14

【Usage Guide】If no interface name is specified, bandwidth utilization information of all interfaces is displayed. The bandwidth here refers to the actual link bandwidth, not the bandwidth configuration value under the interface.

【Configuration Example]】1: Display the port bandwidth utilization information of interface GigabitEthernet 0/1.

Description: Bandwidth is the interface link bandwidth, that is, the maximum rate of the link, and Bandwidth Usage is the current

bandwidth utilization.

```
Interface                          Bandwidth     Bandwidth Usage
_________________________________ _____________ ___________________

GigabitEthernet 0/0                1000000  Kbit 0.001840950%
```

【Prompt Information】-

【Platform Description】-

2 MAC Adress

2.1 clear mac-address-table dynamic

Clear the specified dynamic MAC address, or the dynamic MAC address for the specified interface / VLAN.

clear mac-address-table dynamic [address mac-addr [interface interface-id] [vlan vlan-id] |

{ [interface interface-id] [vlan vlan-id] }]

【Parameter Description】

Parameter	Description
dynamic	Clear all of the dynamic addresses.
address mac-addr	Clear the specified dynamic address
interface interface-id	Clear all of the dynamic addresses for the specified interface.
vlan vlan-id	Clear all dynamic addresses for the specified VLAN, ranging from 1-4094
dynamic	Clear all of the dynamic addresses.

【Command Mode】 Privilege mode

【Default Level】 2

【Usage Guide】 You can use the entire show mac-address-table dynamic command to view the dynamic address table content.

【Configuration Example】 Delete all of the dynamic addresses.

```
AC-FS# clear mac-address-table dynamic
```

【Prompt Information】 -

【Platform Description】 -

2.2 mac-address-learning

Open the MAC address learning function on the interface.

mac-address-learning

Turn off the MAC address learning function on the interface.

no mac-address-learning

Turn off the MAC address learning function on the interface.

default mac-address-learning

【Parameter Description】 -

【Command Mode】 Interface mode

【Default Configuration】 Address learning ability is turned on

【Default Level】 14

【Usage Guide】 MAC address learning capabilities cannot be closed on security ports, and address learning ports cannot configure security functions.

【Configuration Example】 Turn off the interface address learning capability:

```
AC-FS(config-if-interface-id)# no mac-address-learning
```

【Prompt Information】 -

【Platform Description】 -

2.3 mac-address-table aging-time

Set the dynamic address ageing time.

mac-address-table aging-time seconds

Restore the default.

no mac-address-table aging-time

Restore the default.

default mac-address-table aging-time

【Parameter Description】

Parameter	Description
seconds	Dynamic address burn-in time, in seconds. The scope is determined by the equipment.0

	Indicates the closing of the aging work

【Command Mode】 Global configuration mode

【Default Configuration】 The default value is 300 seconds.

【Default Level】 14

【Usage Guide】Use the show mac-address-table aging-time command to view the settings.

【Configuration Example】 The MAC address was aged to 500 seconds.

```
AC-FS(config)#mac-address-table aging-time 500
```

【Prompt Information】 -

【Platform Description】 -

2.4 mac-address-table filtering

Set the filter address within the specified VLAN

mac-address-table filtering mac-address vlan vlan-id

Remove the filter address.

no mac-address-table filtering mac-address vlan vlan-id

Remove the filter address.

default mac-address-table filtering mac-address vlan vlan-id

【Parameter Description】

Parameter	Description
mac-address	Filter address.
vlan-id	VLAN ID, ranging from 1-4094

【Command Mode】 Global configuration mode

【Default Configuration】 No filter addresses are set by default.

【Default Level】 14

【Usage Guide】The filter address cannot be a multicast address.

【Configuration Example】 Specifies that the MAC address 0000.0202.0303 is set to the filter address within the VLAN 3

```
AC-FS(config)#mac-address-table filtering 0000.0202.0303 vlan 3
```

【Verification】 Use the show mac-address-table filtering command to view the filter address settings.

【Prompt Information】 Tip cannot be set to filter the address.

【Common Mistake】 -

【Platform Description】 -

2.5 mac-address-table notification

Open the Learning MAC address notification function, set the time interval for the address notification MIB, and the maximum number recorded in the address notification history table.

mac-address-table notification [interval value | history-size value]

Restore the default.

no mac-address-table notification [interval | history-size]

Restore the default.

default mac-address-table notification [interval | history-size]

【Parameter Description】

Parameter	Description
interval value	Set the time interval for sending the MAC address Trap, the default is 1 second, and the range is 1-3600.
history-size value	The maximum number of table items in the MAC notification history table, the default is 50, and the range is 1-200.

【Command Mode】 Global configuration mode

【Default Configuration】 The default interval is 1 second, and the maximum number of notifications for table item default notifications is 50.

【Default Level】 14

【Usage Guide】The MAC address notification feature is only for dynamic and secure addresses, while changes to static addresses will not produce Trap notifications. You can open or close the functionality of the device for sending the MAC address Trap by using the command snmp-server enable traps mac-notification in global configuration mode

【Configuration Example】 Set the MAC address notification time interval and the maximum number of MAC addresses for each notification.

```
AC-FS(config)# mac-address-table notification AC-FS(config)# mac-
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

2.6 mac-address-table static

Set up a static address

mac-address-table static mac-addr vlan vlan-id interface interface-id

Delete a static address.

no mac-address-table static mac-addr vlan vlan-id interface interface-id

Delete a static address.

default mac-address-table static mac-addr vlan vlan-id interface interface-id

【Parameter Description】

Parameter	Description
mac-addr	Specifies the destination MAC address corresponding to the table item.

vlan-id	Specifies the VLAN corresponding to the table item, ranging from 1-4094.
interface-id	The interface to which the package is forwarded (either a physical port or a Aggregate Port).

【Command Mode】 Global configuration mode

【Default Configuration】 No static address is set by default.

【Default Level】 14

【Usage Guide】 Static address and device learned dynamic address function are the same. Compared to dynamic addresses, static addresses are never aged and can only be configured and removed manually; even if the device is reset. A static address cannot be set to a multicast address. Use the show mac-address-table static command to view the static address table settings.

【Configuration Example】 -

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

2.7 show mac-address-learning

View the port address learning capability

show mac-address-learning

【Parameter Description】-

【Command Mode】 All patterns

【Default Level】 2

【Usage Guide】 -

【Configuration Example】 Displays the port address learning capability:

```
AC-FS(config)#show mac-address-learning GigabitEthernet 0/0
learning ability: disable GigabitEthernet 0/1     learning ability:
enable GigabitEthernet 0/2      learning ability: enable
GigabitEthernet 0/3      learning ability: enable
```

【Prompt Information】 -

【Platform Description】 -

2.8 show mac-address-table

Displays all types of MAC address information (including dynamic addresses, static addresses, and filter addresses).

show mac-address-table [address mac-addr] [interface interface-id] [vlan vlan-id]

【Parameter Description】

Parameter	Description
address mac-addr	Specified MAC address.
interface interface-id	Interface ID.
vlan vlan-id	VLAN, the range from 1-4094.

【Command Mode】 all mode

【Default Level】 2

【Usage Guide】 -

【Configuration Example】 View the MAC address table:

```
AC-FS# show mac-address-table address 00d0.f800.1001
Vlan        MAC Address          Type   Interface
--------    --------------       --------   --------

1           00d0.f800.1001       STATIC  GigabitEthernet 1/1
```

【Field interpretation】

Field	Interpretation:
Vlan	Interface address.
MAC Address	MAC address.
Type	MAC address type.

【Prompt Information】 -

【Platform Description】 -

2.9 show mac-address-table aging-time

Displays the dynamic address aging time.

show mac-address-table aging-time

【Parameter Description】-

【Command Mode】 all mode

【Default Level】 2

【Usage Guide】 -

【Configuration Example】 View the aging time of the MAC address.

```
AC-FS# show mac-address-table aging-time
Aging time    : 300
```

【Prompt Information】 -

【Platform Description】 -

2.10 show mac-address-table count

Displays the statistics on the number of address table items in the address table

show mac-address-table count [interface interface-id | vlan vlan-id]

【Parameter Description】

Parameter	Description
interface interface-id	Interface ID.
vlan vlan-id	VLAN, the range from 1-4094.

【Command Mode】 Privilege mode

【Default Level】 2

【Usage Guide】show mac-address-table count, count the number of table items according on the type of MAC address table items;

show mac-address-table count interface, number of interface table items according to MAC address table items;

show mac-address-table count vlan, number of VLAN statistical items according to the MAC address table item.

【Configuration Example】 1: Displays the number of table items for each type of the MAC address:

```
AC-FS# show mac-address-table count
Dynamic Address Count  : 51
Static  Address  Count  :  0  Filter
Address  Count  :  0  Total  Mac
Addresses    : 51
Total Mac Address Space Available: 8139
```

2: Displays the number of MAC addresses under the VLAN 1 ：

```
AC-FS# show mac-address-table count vlan 1
Dynamic Address Count  : 7
Static Address Count : 0 Filter
Address Count  : 0
Total Mac Addresses       :7
```

3: Displays the number of MAC addresses under interface g0 / 1：

```
AC-FS# show mac-address-table interface g0/1 Dynamic
Address Count : 10
Static  Address Count  : 0
Filter Address Count : 0 Total
Mac Addresses             :10
```

【Field interpretation】

Field	Interpretation:
Dynamic Address Count	Number of dynamic MAC addresses.
Static Address Count	Number of static MAC addresses.
Filter Address Count	Filter the number of addresses.

Total Mac Addresses	Total number of MAC addresses.

【Prompt Information】 -

【Platform Description】 -

2.11 show mac-address-ttable dynamic

Displays the dynamic address table information, which can be viewed by the MAC address, interface, and VLAN.

show mac-address-table dynamic [address mac-addr] [interface interface-id] [vlan vlan-id]

【Parameter Description】

Parameter	Description
mac-addr	Specifies the destination MAC address corresponding to the table item.
vlan-id	Specifies the VLAN corresponding to the table item, ranging from 1-4094.
interface-id	The interface to which the package is forwarded (either a physical port or a AggregatePort).

【Command Mode】 all mode

【Default Level】 2

【Usage Guide】 -

【Configuration Example】 View all of the dynamic MAC address tables

```
AC-FS# show mac-address-table dynamic
Vlan    MAC Address       Type        Interface
----    --------------    -------     --------------------
1    0000.0000.0001     DYNAMIC  GigabitEthernet 1/1
1..... 0001.960c.a740     DYNAMIC  GigabitEthernet 1/1
1..... 0007.95c7.dff9     DYNAMIC  GigabitEthernet 1/1
1..... 0007.95cf.eee0     DYNAMIC  GigabitEthernet 1/1
1..... 0007.95cf.f41f     DYNAMIC  GigabitEthernet 1/1
1..... 0009.b715.d400     DYNAMIC  GigabitEthernet 1/1
1..... 0050.bade.63c4     DYNAMIC  GigabitEthernet 1/1
```

【Field interpretation】

Field	Interpretation
Vlan	The VLAN where the MAC address is located.
MAC Address	MAC address.
Type	MAC address type.
Interface	Interface of the MAC address.

【Prompt Information】 -

【Platform Description】 -

2.12 show mac-address-table filtering

Displays the filter address table information.

show mac-address-table filtering [addr mac-addr] [vlan vlan-id]

【Parameter Description】

Parameter	Description
mac-addr	Specifies the destination MAC address corresponding to the table item.
vlan-id	Specifies the VLAN corresponding to the table item, ranging from 1-4094.

【Command Mode】 Privilege mode

【Default Level】 2

【Usage Guide】 -

【Configuration Example】 View the filter address table.

```
AC-FS# show mac-address-table filtering
Vlan      MAC Address          Type     Interface
_____     ___________________  _______  ___________
1      0000.2222.2222          FILTER   Not available
```

【Field interpretation】

Field	Interpretation:

Vlan	The VLAN where the MAC address is located.
MAC Address	MAC address.
Type	MAC address type.
Interface	Interface of the MAC address.

【Prompt Information】 -

【Platform Description】 -

2.13 show mac-address-table interface

Displays all types of address information (including dynamic addresses, static addresses) for the specified interface.

【Parameter Description】

Parameter	Description
interface-id	Specified interface (either a physical port or, AggregatePort).
vlan-id	Specifies the VLAN corresponding to the table item, ranging from 1-4094.

【Command Mode】 Privilege mode

【Default Level】 2

【Usage Guide】 -

【Configuration Example】 View the MAC address on the specified interface.

```
AC-FS# show mac-address-table interface GigabitEthernet 1/1 Vlan
MAC Address        Type   Interface                                1
00d0.f800.1001     STATIC   GigabitEthernet 1/1
1        00d0.f800.1002     STATIC    GigabitEthernet 1/1
1        00d0.f800.1003     STATIC    GigabitEthernet 1/1
1        00d0.f800.1004     STATIC    GigabitEthernet 1/1
```

【Field interpretation】

Field	Interpretation:
Vlan	The VLAN where the MAC address is located.
MAC Address	MAC address.
Type	MAC address type.
Interface	Interface of the MAC address.

【Prompt Information】 -

【Platform Description】 -

2.14 show mac-address-table notification

Displays the MAC address notification function settings and the notification table information.

show mac-address-table notification [interface [interface-id] | history]

【Parameter Description】

Parameter	Description
interface	Displays the MAC notification function settings on all of the interfaces.
interface-id	Displays the MAC notification function settings on the specified interface.
history	Displays the MAC notification history table information.

【Command Mode】 Privilege mode

【Default Level】 2

【Usage Guide】 -

【Configuration Example】 View the global configuration information for the MAC address notification feature.

```
AC-FS#show mac-address-table notification MAC
Notification Feature : Enabled Interval(Sec):
300 Maximum History Size : 50
Current History Size : 0
```

【Field interpretation】

Field	Interpretation:

Interval (Sec)	Time interval for announcing the MAC address.
Maximum History Size	Maximum number of table items for the MAC Address Notification history table.
Current History Size	The number of current record entries.

【Prompt Information】 -

【Platform Description】 -

2.15 show mmac-address-table static

Displays the static address。

show mac-address-table static [addr mac-addr] [interface interface-id] [vlan vlan-id]

【Parameter Description】

Parameter	Description
mac-addr	Specifies the destination MAC address corresponding to the table item.
vlan-id	Specifies the VLAN corresponding to the table item, ranging from 1-4094.
interface-id	Interface to which the package is forwarded (either a physical port or a Aggregate Port).

【Command Mode】 Privilege mode

【Default Level】 2

【Usage Guide】 -

【Configuration Example】 Displays all of the static address information：

```
AC-FS# show mac-address-table static
Vlan    MAC Address       Type        Interface
----    -----------       --------    ---------------------
1    00d0.f800.1001    STATIC   GigabitEthernet 1/1
1    00d0.f800.1002    STATIC    GigabitEthernet 1/1
1    00d0.f800.1003    STATIC    GigabitEthernet 1/1
```

【Field interpretation】

Field	Interpretation:
Vlan	The VLAN where the MAC address is located.

MAC Address	MAC address.
Type	MAC address type.
Interface	Interface of the MAC address.

【Prompt Information】 -

【Platform Description】 -

2.16 show mac-address-table vlan

Displays all types of address information for the specified VLAN

show mac-address-table vlan [vlan-id

【Parameter Description】

Parameter	Description
vlan-id	Specified VLAN ID, the range from 1-4094.

【Command Mode】 Privilege mode

【Default Level】 2

【Usage Guide】 -

【Configuration Example】 View the MAC address in the VLAN 1:

```
AC-FS# show mac-address-table vlan 1
Vlan    MAC Address       Type        Interface
------  ------------      ------  ------------------  1
00d0.f800.1001    STATIC   GigabitEthernet 1/1
1     00d0.f800.1002     STATIC     GigabitEthernet 1/1
```

【Field interpretation】

Field	Interpretation:
Vlan	The VLAN where the MAC address is located.
MAC Address	MAC address.
Type	MAC address type.

Interface	Interface of the MAC address.

【Prompt Information】 -

【Platform Description】 -

2.17 snmp trap mac-notification

Open the MAC address notification function for the interface

snmp trap mac-notification { added | removed }

Close this feature.

no snmp trap mac-notification { added | removed }

Close this feature.

default snmp trap mac-notification { added | removed }

【Parameter Description】

Parameter	Description
added	Notify when the address increases.
removed	Notify when the address is deleted.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 View the settings by using the show mac-address-table notification interface command.

【Configuration Example】 1. Turn on the switch that notifies the trap when the MAC address is increased on the port.

```
AC-FS(config)# interface GigabitEthernet 1/1
AC-FS(config-if-GigabitEthernet 1/1)# snmp trap mac-notification added
```

2. Turn on the switch that notifies the trap when the MAC address is deleted on the port.

```
AC-FS(config)# interface GigabitEthernet 1/1
AC-FS(config-if-GigabitEthernet 1/1)# snmp trap mac-notification removed
```

【Prompt Information】 -

【Platform Description】 -

3 VLAN

3.1 add

Adds one or a group of Access interfaces to the current VLAN.

add interface { interface-id | range interface-range }

Removes an Access interface or group of Access interfaces from the current VLAN.

no add interface { interface-id | range interface-range }

Removes an Access interface or group of Access interfaces from the current VLAN.

default add interface { interface-id | range interface-range }

【Parameter Description】

Parameter	Description
Interface-id	Ethernet interface or AP port on the second floor.
Range interface-range	Ethernet interface range on the second floor or AP port range on the AP.

【Default Configuration】 All second-floor Ethernet interfaces belong to VLAN1.

【Command Mode】VLAN, Config mode

【Default Level】 14

【Usage Guide】 The command is valid for the Access ports only. The configuration effect of this command is the same as the command (switchport access vlan vlan-id) that specifies the VLAN to which the interface belongs in interface mode; for the VLAN command, the configuration principle is that the post configured command overrides the previously configured command. When using this command to add the second-floor AP port to the current VLAN, the configuration is only valid for the second-floor AP port and is invalid for the member port of the second-floor AP port. When using this command to add the second-floor AP port to the current VLAN, the configuration works only for the second-floor AP port and not for the member port of the second-floor AP port.

【Configuration Example】 1. Add the GigabitEthernet 0 / 10 interface to the VLAN20.

```
AC-FS# configure terminal AC-
FS (config)#vlan 20
AC-FS (config-vlan)#add interface GigabitEthernet 0/10 AC-FS
(config-vlan)#show int g 0/10 sw
Interface                        Switchport Mode      Access Native Protected VLAN lists
_______________________________ __________ _________ ______ ______ _________ __________

GigabitEthernet 0/10             enabled    ACCESS    20     1      Disabled  ALL
```

2. Add the GigabitEthernet 0 / 1 to GigabitEthernet 0 / 10 interface to the VLAN200.

```
AC-FS# configure terminal
```

```
AC-FS# configure terminal AC-
FS (config)#vlan 20
AC-FS (config-vlan)#add interface GigabitEthernet 0/10 AC-FS
(config-vlan)#show int g 0/10 sw
Interface                        Switchport Mode      Access Native Protected VLAN lists
_______________________________ __________ _________ ______ ______ _________ __________

GigabitEthernet 0/10             enabled    ACCESS    20     1      Disabled  ALL
```

3: Add the AggregatePort 10 port to the VLAN20.

```
AC-FS# configure terminal
SwitchA(config)#vlan 20
SwitchA(config-vlan)#add interface aggregateport 10 AC-
FS# show interface aggregateport 10 switchport
Interface  Switchport   Mode  Access  Native Protected  VLAN lists
__________  ________       _____  _____  ____ __________ _______

AggregatePort 10 enabled  ACCESS  20   1   Disabled  ALL
```

【Verification】 Use show vlan to see if the port is only within the joined VLAN.

【Prompt Information】 -

【Common Mistake】 1: The added interface is not a second-floor intersection.

2: The added interface is not a Access port.

3: The joined interface is the AP member port.

【Platform Description】 -

3.2 name

Set the name of the VLAN.

name vlan-name

Recover to a default value.

no name

Recover to a default value.

default name

【Parameter Description】

Parameter	Description
vlan-name	the name of the VLAN

【Default Configuration】 The VLAN default name is VLAN + VLAN ID, such as the VLAN 2 default name is "VLAN0002".

【Command Mode】 VLAN, Config mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example】 Set the name of the VLAN 10:

```
AC-FS(config)# vlan 10
AC-FS(config-vlan)# name vlan10
```

【Verification】 Use the show vlan command to view the vlan configuration.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

3.3 show vlan

Displays information such as the member ports of the VLAN.

show vlan [id vlan-id]

【Parameter Description】

Parameter	Description
VLAN-ID	The number of VLAN ID.

【Command Mode】 All patterns

【Default Level】 2

【Usage Guide】 -

【Configuration Example】 1. View the configuration of the VLAN 1 and the exchange ports within the VLAN 1

```
AC-FS(config-vlan)#show vlan id 20
VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------------

  20 VLAN0020                            STATIC    Gi0/1
```

2. View all the configurations of the VLAN and the exchanges within the VLAN.

```
AC-FS(config-vlan)#show vlan
VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------------

   1 VLAN0001                            STATIC    Gi0/1, Gi0/2, Gi0/4, Gi0/5
                                                   Gi0/6, Gi0/7, Gi0/8, Gi0/9
                                                   Gi0/10, Gi0/11, Gi0/12, Gi0/13
                                                   Gi0/14, Gi0/15, Gi0/16, Gi0/17
                                                   Gi0/18, Gi0/19, Gi0/20, Gi0/21
                                                   Gi0/22, Gi0/23, Gi0/24
   2 VLAN0002                            STATIC    Gi0/1
  20 VLAN0020                            STATIC    Gi0/1
```

【Field interpretation:】

Field	Instruction
VLAN	VLAN ID.
Name	VLAN Name.
Status	Attributes of VLAN: Dynamic, Static, Super VLAN, etc.
Ports	Ports that belong to this VLAN.

【Prompt Information】 -

【Platform Description】 -

3.4 switchport access

Add a access port to the specified VLAN.

switchport access vlan vlan-id

Restore the Default Configuration.

no switchport access vlan

Restore the Default Configuration.

default switchport access vlan

【Parameter Description】

Parameter	Description
vlan-id	The ID of the VLAN that the port wants to join.

【Default Configuration】 The Access port default only joins the VLAN 1.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 If the added VLAN does not exist, a VLAN is created first, and then the port is added to the VLAN; if the VLAN already exists, the port is added to the specified VLAN. You cannot do if the port is a trunk port.

【Configuration Example】 Configure the port, the access VLAN.

```
AC-FS(config)# interface gigabitEthernet 0/1
AC-FS(config-if-GigabitEthernet 0/1)# switchport access vlan 2
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

3.5 switchport mode

Specify the mode for a two-level interface (switch port) that can be designated as a access port, trunk port, hybrid port, uplink port, or set up as a 802.1Q tunnel. switchport mode { access | trunk | hybrid | uplink }

Restore the mode of the interface to the default value.

no switchport mode

Restore the mode of the interface to the default value.

default switchport mode

【Parameter Description】

Parameter	Description
access	Set a switch port to access port.
trunk	Set a switch port to trunk port.
hyhrid	Set a switch port to hybrid port.
uplink	Set a switch port to uplink port.

【Default Configuration】 The switch port default mode is access.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】If a switch port mode is access, the interface is only a member of a VLAN. You can use the switchport access vlan. The command specifies that the interface is a member of a certain VLAN. If a switch port mode is trunk, all VLAN are added by default, you can also add the port in / exit the specified VLAN by the command switchport trunk allowed. If a switch port pattern is uplink, the default also adds all VLAN. Unlike Trunk ports, uplink port output messages with Tag, namely Tag that does not strip the default VLAN If a switch port mode is hybrid, the default also adds all VLAN, unlike the Trunk port, it can be passed by command. The switchport hybrid allowed specifies that the port is joined as a Tag or a UNTag.

【Configuration Example】 1: Set port 1 to the access port

```
AC-FS(config)#int g 0/1
AC-FS(config-if-GigabitEthernet 0/1)#switchport mode access
```

2: Set port 1 to the trunk port

```
AC-FS(config)#int g 0/1
AC-FS(config-if-GigabitEthernet 0/1)# switchport mode trunk
```

3: Set port 1 to the uplink port

```
AC-FS(config)#int g 0/1
AC-FS(config-if-GigabitEthernet 0/1)# switchport mode uplink
```

4: It port 1 to the hybrid port

```
AC-FS(config)#int g 0/1
AC-FS(config-if-GigabitEthernet 0/1)# switchport mode hybrid
```

【Verification】 It can be viewed with the show interface switch command.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

3.6 switchport hybrid allowed

Add the port to the specified VLAN list in a Tag or UNTag, or exit the port from the specified VLAN list.

switchport hybrid allowed vlan { { [add | only] tagged vlist | [add] untagged vlist } | remove vlist }

Restore the hybrid port to the default properties.

no switchport hybrid allowed vlan

Restore the hybrid port to the default properties.

no switchport hybrid allowed vlan

【Parameter Description】

Parameter	Description
add	Add the port to the VLAN, not specified
only	Add the port to the VLAN an d exit the VLAN that is not in the VLAN list not specified.
Tagged	Add the port to the specified VLAN as a Tag, and the band of the VLAN message is output from the port tag.
untagged	Add the port to the specified VLAN as a UN tag, and the message of the VLAN is output from it.

【Default Configuration】 The default hybrid port belongs to all VLAN, the port adds all VLAN other than VLAN in default in Tag, and the default VLAN in UNTag.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 If the added VLAN does not exist, a VLAN is created first, and then the port is added to the VLAN; if the VLAN already exists, the port is added to the specified VLAN. You cannot do if the port is a trunk port.

【Configuration Example】 1: Add the hybrid port to the VLAN 20 and VLAN30 as a UNTag:

```
AC-FS(config)# interface gigabitEthernet 0/1
AC-FS(config-if-GigabitEthernet 0/1)# switchport mode hybrid
AC-FS(config-if-GigabitEthernet 0/1)#switchport hybrid allowed vlan untagged 20 AC-
FS(config-if-GigabitEthernet 0/1)#switchport hybrid allowed vlan add untagged 30
```

2: Add the hybrid port to VLAN 40 and VLAN 50 in a Tag:

```
AC-FS(config)# interface gigabitEthernet 0/1 AC-FS(config-if-
GigabitEthernet 0/1)#switchport mode hybrid
AC-FS(config-if-GigabitEthernet 0/1)#switchport hybrid allowed vlan tagged 40
AC-FS(config-if-GigabitEthernet 0/1)#switchport hybrid allowed vlan tagged 50
```

3: Remove the hybrid port from the VLAN 20:

```
AC-FS(config)# interface gigabitEthernet 0/1 AC-FS(config-if-
GigabitEthernet 0/1)#switchport mode hybrid
AC-FS(config-if-GigabitEthernet 0/1)#switchport hybrid allowed vlan remove 20
```

4: The hybrid port was added to the VLAN 20 as a Tag, while all other VLAN were removed:

```
AC-FS(config)# interface gigabitEthernet 0/1 AC-FS(config-if-
GigabitEthernet 0/1)#switchport mode hybrid
AC-FS(config-if-GigabitEthernet 0/1)#switchport hybrid allowed vlan only tagged 20
```

【Verification】 View it via show interface [intf-id].

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

3.7 switchport hybrid native

Specifies the default VLAN for the hybrid port.

switchport hybrid native vlan vlan-id

Restore the default value.

no switchport hybrid native vlan

Restore the default value.

default switchport hybrid native vlan

【Parameter Description】

Parameter	Description
vlan-id	Specified the default VLAN for the hybrid port without messages within the default

	VLAN are exported from that inface.

【Default Configuration】 The default Native VLAN is the VLAN 1.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 After assigning the native vlan, the native vlan's message is exported from the hybrid port without a Tag. When coming in from the hybrid mouth without a Tag message recognize For it is native vlan's message.

【Configuration Example】 Set the native vlan of the hybrid port Gigabit Ethernet 0 / 1 port to VLAN 20

```
AC-FS(config-if-GigabitEthernet 0/1)#interface gigabitEthernet 0/1
AC-FS(config-if-GigabitEthernet 0/1)#switchport mode hybrid AC-
FS(config-if-GigabitEthernet 0/1)#switchport hybrid native vlan 20
```

【Verification】 View the configuration on the interface via the show running-config.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

3.8 switchport trunk allowed vlan

Add a trunk port or uplink port to / exit a specified VLAN.

switchport trunk allowed vlan { all | { add vlan-list | remove vlan-list | except vlan-list | only vlan-list } }

Restore the Default Configuration.

no switchport trunk allowed vlan

Restore the Default Configuration.

default switchport trunk allowed vlan

【Parameter Description】

Parameter	Description
all	Add trunk port to all VLANs.
add	Add the trunk port to the specified VLAN list.
remove	Remove the trunk port from the specified VLAN list.
except	Remove the trunk port from the specified VLAN list, and add the port to all other VLANs except the VLAN list.
only	Add the trunk port to the specified VLAN list, and remove the port from all other VLANs except the VLAN list.
vlan-list	List of VLANs for the specified operation.

【Default Configuration】 By default, the trunk and uplink ports belong to all VLAN.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 A trunk / uplink port by default transmits traffic to all the VLAN (1-4094) supported by this device. However, you can also go through it by setting it up. The licensed VLAN list of the trunk / uplink port cannot limit the traffic to certain VLAN through this trunk / uplink port. Use the show interfaces command to view the settings.

【Configuration Example】 1: Below is one removing the VLAN 2 from the trunk port Gigabit Ethernet 0 / 10:

```
AC-FS(config)# interface gigabitEthernet 0/10
AC-FS(config-if-GigabitEthernet 0/10)# switchport mode trunk
AC-FS(config-if-GigabitEthernet 0/10)# switchport trunk allowed vlan remove 2
```

2: Below, add the trunk port G 0 / 10 to a VLAN other than VLAN 10 ：

```
AC-FS(config)# interface gigabitEthernet 0/10
AC-FS(config-if-GigabitEthernet 0/10)# switchport trunk allowed vlan except 10
```

3: Below, add the trunk port G 0 / 10 to the VLAN 10 and remove the other VLAN：

```
AC-FS(config)# interface gigabitEthernet 0/10
AC-FS(config-if-GigabitEthernet 0/10)# switchport trunk allowed vlan only 10
```

4: Below is the removal of the uplink port GigabitEthernet 0 / 10 port from the VLAN 10 ：

```
AC-FS(config)# interface gigabitEthernet 0/10
AC-FS(config-if-GigabitEthernet 0/10)# switchport mode uplink
AC-FS(config-if-GigabitEthernet 0/10)# switchport trunk allowed vlan remove 10
```

5: Below, add the uplink port GigabitEthernet 0 / 10 to a VLAN other than VLAN 10 ：

```
AC-FS(config)# interface gigabitEthernet 0/10
AC-FS(config-if-GigabitEthernet 0/10)# switchport trunk allowed vlan except 10
```

6: Below, add the uplink port G 0 / 10 port to the VLAN 10 and remove the other VLAN：

```
AC-FS(config)# interface gigabitEthernet 0/10
AC-FS(config-if-GigabitEthernet 0/10)# switchport trunk allowed vlan only 10
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

3.9 switchport trunk native vlan

Specifies the default VLAN for the trunk / uplink port.

switchport trunk native vlan vlan-id

Restore the Default Configuration.

no switchport trunk native vlan

Restore the Default Configuration.

default switchport trunk native vlan

【Parameter Description】

Parameter	Description
add	Specified native VLAN ID's.

【Default Configuration】 By default, the default VLAN for the trunk / uplink is VLAN 1.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 After assigning the native vlan of the trunk port, the message without Tag is the native vlan message by default; the message within the native vlan is from the trunk The Tag of the message is stripped as the mouth goes out.

【Configuration Example】1: Specifying that the native vlan of the trunk port GigabitEthernet 0 / 10 port is VLAN 10:

```
AC-FS(config)#interface gigabitEthernet 0/10
AC-FS(config-if-GigabitEthernet 0/10)# switchport mode trunk AC-
FS(config-if-GigabitEthernet 0/10)# switch trunk native vlan 10
```

2: Specifying that the native vlan of the trunk port GigabitEthernet 0 / 10 port is VLAN 10:

```
AC-FS(config)#interface gigabitEthernet 0/10
AC-FS(config-if-GigabitEthernet 0/10)# switchport mode uplink AC-
FS(config-if-GigabitEthernet 0/10)# switch trunk native vlan 10
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

3.10 vlan

Create a VLAN or go into the VLAN mode.

vlan { vlan-id | range vlan-range }

Delete the already existing VLAN.

no vlan { vlan-id | range vlan-range }

Restore the specified already existing VLAN to a normal static VLAN.

default vlan { vlan-id | range vlan-range }

【Parameter Description】

Parameter	Description
VLAN-ID	The vlan id no. Note the default VLAN (VLAN 1) is not delete.
VLAN-rang	The VLAN ID rang is available.

【Default Configuration】 Normal Static, VLAN

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】 Create the VLAN 10 and go into the VLAN 10 mode.

```
AC-FS(config)# vlan 10
AC-FS(config-vlan)#
```

【Verification】 -

【Prompt Information】-

【Common Mistake】 -

【Platform Description】 -

3.11 bridge-l2-isolation

Turn off the second-floor isolation function of the physical switch port in the VLAN.

no bridge-l2-isolation

Turn on the second-floor isolation function of the physical exchange port in the VLAN.

bridge-l2-isolation

【Parameter Description】-

【Default Configuration】 For the equipment with the second isolation function, by default, the second isolation function is switched on, that is, the physical exchange ports in the same VLAN; for the equipment that does not support the second isolation function, the physical exchange ports in the same VLAN can communicate between the two floors. The show bridge-l2-isolation command allows you to see whether the device knows if it supports second-layer isolation functions, or so, if the command does.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example】 1. Turn off the second-floor isolation function of the device.

```
AC-FS(config)# no bridge-l2-isolation
```

2. Turn on the second-floor isolation function of the device.

```
AC-FS(config)# bridge-l2-isolation
```

【Verification】 Use the show bridge-l2-isolation command to see whether the current device supports second-layer isolation, and to view the second-floor isolation configuration status of the device.

【Prompt Information】 -

【Common Mistake】 -

【 Platform Description 】 The second floor isolation feature is currently only supported for AP aggregate, and is currently only supported on AP devices that support AP aggregate gate. In addition, although in the thin AP scenario, the configuration before the restart is not saved after the restart on the AP, the isolated configuration on the second floor can be consistent with the restart of the device.

4 Super VLAN

4.1 show super vlan

View the configuration for all Super VLAN and Sub VLAN s.

show supervlan

View the configuration of the specified Super VLAN and its Sub VLAN s.

show supervlan [vlan-id]

【Parameter Description】

Parameter	Description
VLAN-ID	It must be Super VLAN's VLAN ID.

【Command Mode】 All patterns

【Default Level】 14

【Usage Guide】 Use this command to view the correspondence and other information between the Super VLAN and its Sub VLAN.

【Configuration Example】 1: View the configuration of the specified Super VLAN .

```
SwitchA(config-if-range)# show supervlan 2
supervlan id  supervlan  subvlan id  subvlan  subvlan ip range
------------  ----------  ----------  -------  ---------------
           2          ON          10       ON  192.168.196.10 - 192.168.196.50
                          20       ON  192.168.196.60 - 192.168.196.100
                          30       ON  192.168.196.110 - 192.168.196.150
```

2: View the configuration of all Super VLAN s.

```
SwitchA(config-if-range)# show supervlan
supervlan id  supervlan  subvlan id  subvlan  subvlan ip range
------------  ----------  ----------  -------  ----------------
           2          ON          10       ON  192.168.196.10 - 192.168.196.50
                                  20       ON  192.168.196.60 - 192.168.196.100
                                  30       ON  192.168.196.110 - 192.168.196.150
           6          ON          7        ON
                                  8        ON
```

【Verification】 Use the show bridge-l2-isolation command to see whether the current device supports second-layer isolation, and to view the second-floor isolation configuration status of the device.

【Field Interpretation】

Field	Instruction
supervlan id	Super VLAN Master VLAN ID.
subvlan id	Sub VLAN of the VLAN ID.
subvlan ip range	Sub VLAN for IP address range.

【Prompt Information】 -

【Platform Description】 -

4.2 subvlan

Configure the Sub VLAN.

subvlan [vlan-id-list]

Cancel the Sub VLAN.

no subvlan [vlan-id-list]

Restore the Default Configuration.

default subvlan [vlan-id-list]

【Parameter Description】

Parameter	Description
VLAN-ID-list	Specify the Sub VLAN for the Super VLAN.

【Default Configuration】 Common VLAN

【Command Mode】 VLAN pattern

【Default Level】 14

【Usage Guide】 The VLAN that needs to use the same network segment will all be divided to the Sub VLAN of a Super VLAN.

【Configuration Example】 1: Use the subvlan command to add the specified Sub VLAN.

```
SwitchA(config)#vlan 2
SwitchA(config-vlan)#supervlan
SwitchA(config-vlan)#subvlan 10,20,30
```

2: Remove the specified Sub VLAN by using the no command.

```
SwitchA(config)#vlan 2
SwitchA(config-vlan)#no subvlan 30
```

3: Use the default command to remove the specified Sub VLAN.

```
SwitchA(config)#vlan 2
SwitchA(config-vlan)#default subvlan 30
```

4: Use the default command to remove all Sub VLAN s.

```
SwitchA(config)#vlan 2
SwitchA(config-vlan)#default subvlan
```

【Verification】 Use the show supervlan [vlan-id] command to view the Sub VLAN configuration for the specified Super VLAN.

【Prompt Information】1: An error is prompted if the VLAN mode is not a Super VLAN.

```
vlan 10 is not a supervlan
```

2: If the VLAN configured is not a static VLAN and a dynamic VLAN, error.

```
The vlan is dynamic vlan
```

3: When configuring a Sub VLAN, if its Super VLAN has already configured the SVI, each Sub VLAN is assigned a triple port that is invisible to the user, and the setting may fail due to insufficient resources。

```
the vlan can't be set as subvlan for lack of resources
```

【Common Mistake】 1: Configure that a VLAN is not present to be a Sub VLAN.

2: The Sub VLAN is not configured in the VLAN mode of the Super VLAN.

3: Sub VLAN overlap for different Super VLAN.

4: VLAN has already configured VLAN triple ports, and its configuration to Sub VLAN will fail.

5: Configure the dynamic VLAN to be a Sub VLAN.

【Platform Description】 -

4.3 subvlan-address-range start-ip end-ip

Configure the user IP address range within the Sub VLAN .

subvlan-address-range start-ip end-ip

Cancel the IP address range for the Sub VLAN .

no subvlan-address-range

Restore the Default Configuration.

default subvlan-address-range

【Parameter Description】

Parameter	Description
Start-ip	The starting value of the IP range.
end-ip	Maximum value of IP range.

【Default Configuration】 No IP address scope exists.

【Command Mode】 VLAN pattern

【Default Level】 14

【Usage Guide】 After the IP address range is configured, the IP address within Sub VLAN cannot communicate if not within that range.

【Configuration Example】 Set the Sub VLAN IP address range.

```
AC-FS(config)# vlan 2
AC-FS(config-vlan)#subvlan-address-range 192.168.23.1 192.168.23.5
```

【Verification】 Use the show supervlan [vlan-id] command to view the configuration of the specified Super VLAN.

【Prompt Information】 -

【Common Mistake】 1: Configure the dynamic VLAN to be a Super VLAN, resulting in a configuration failure.

2: The configured IP address range is not in the segment of the Super VLAN Gateway.

【Platform Description】 -

4.4 supervlan

Configure Super VLAN.

supervlan

Cancel the Super VLAN and restore the Default Configuration.

no supervlan

Restore Default Configuration.

default supervlan

【Parameter Description】-

【Default Configuration】 Normal VLAN.

【Command Mode】VLAN mode

【Default Level】 14

【Usage Guide】 Only the existing VLAN can be configured as Super VLAN.

After configuring the Super VLAN, if the VLAN is not configured with a VLAN Layer 3 port, you need to configure a VLAN Layer 3 port SVI for the Super VLAN.

and IP address so that its Sub VLAN can communicate across VLANs.

There is no physical port in the Super VLAN.

VLAN 1 cannot be configured as a Super VLAN.

A Super VLAN cannot be used as a Sub VLAN of other Super VLANs. Similarly, Sub VLAN cannot be configured as Super VLAN.

【Configuration Example】 1: Configure VLAN as Super VLAN.

```
AC-FS(config)# vlan 2
AC-FS(config-vlan)#supervlan
```

【Verification】 1: Use the show supervlan [vlan-id] command to view the configuration of the specified Super VLAN.

【Prompt Information】 1: If the VLAN is already a Sub VLAN of other VLANs.

```
the vlan is other supervlan's subvlan
```

【Common Mistake】

【Platform Description】 -

5 MSTP

5.1 bpdu src-mac-check

Opens a bpdu source mac check for an interface.

bpdu src-mac-check H.H.H

Turn off the bpdu source mac check function for the interface.

no bpdu src-mac-check

【Parameter Description】

Parameter	Description
H.H.H	Indicates that only bpdu frames whose source mac address is this address are received.

【Default Configuration】 The default is closed.

【Command Mode】 Interface mode

【Default Level】 15

【Usage Guide】 The BPDU source MAC check is used to prevent MSTP from working properly by maliciously attacking the switch by artificially sending BPDU messages. When a switch connected to a port peer-to-peer point-end link is determined, configure the BPDU source MAC check to only receive BPDU frames and discard all the other BPDU frames, thus achieving the purpose of preventing malicious attacks. You can configure the corresponding MAC address for the BPDU source MAC check for a specific port down in interface mode, and only one port allows for one filter MAC address.

【Configuration Example】 Configure interface Gi 1 / 1 receives only bpdu frames where the source mac is 00d0.f800.1e2f.

```
AC-FS(config)# interface gigabitethernet 1/1
AC-FS(config-if-interface-id-interface-id)# bpdu src-mac-check 00d0.f800.1e2f
```

【Verification】 Use the show running-config command to let you see if the command is set.

【Prompt Information】 If the VLAN is already the Sub VLAN for any other VLAN .The vlan is other supervlan's subvlan.

【Common Mistake】 Setting up the BPDU source MAC address check is to receive only the BPDU frame sent by the source MAC address, rather than filtering out the BPDU frame sent by the source MAC address.

【Platform Description】 -

5.2 bridge-frame forwarding protocol bpdu

Open the BPDU transmission function.

bridge-frame forwarding protocol bpdu

Turn off the BPDU transmission function.

no bridge-frame forwarding protocol bpdu

【Parameter Description】-

【Default Configuration】 The default is closed.

【Command Mode】 Interface mode

【Default Level】 15

【Usage Guide】 In the IEEE 802.1Q standard, the destination MAC address of the BPDU 01-80-C2- -00-00-00 is used as a reserved address, where the device following the IEEE 802.1Q standard is not forwarded for the received BPDU frame. However, in actual network distribution, devices may be required to support transmission BPDU frames. For example, when a device is not turned on the STP protocol, the BPDU frame is required so that the generation tree calculation between the connected devices is normal.

The BPDU transmission function only works when the STP protocol is turned off. When the STP protocol is on, the device does not transmit the BPDU frame.

【Configuration Example】 Open the BPDU transmission function.

```
AC-FS(config)# bridge-frame forwarding protocol bpdu
```

【Verification】 Use the show running-config command to let you see if the command is set.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.3 clear spanning-tree counters

Clear the packet statistics for the STP

clear spanning-tree counters [interface interface-id]

【Parameter Description】

Parameter	Description
interface-id	corresponding interface.

【Command Mode】 Privilege mode

【Default Level】 15

【Usage Guide】 This command is used to clear the packet statistics for the STP.

【Configuration Example】 1: Clear the packet statistics for the STP.

```
AC-FS# clear spanning-tree counters
```

2: Clear the transceiver packet statistics for the interface Gi 0 / 1.

```
AC-FS# clear spanning-tree counters interface gigabitethernet 0/1
```

【Prompt Information】

【Platform Description】 -

5.4 clear spanning-tree detected-pprotocols

Force the interface to RSTP BPDU and check on BPDU frames.

clear spanning-tree detected-protocols [interface interface-id]

【Parameter Description】

Parameter	Description

interface-id	corresponding interface.

【Command Mode】 Privilege mode

【Default Level】 15

【Usage Guide】 This command uses to force the interface to send RSTP BPDU frames.

【Configuration Example】 Force version checks on all ports

```
AC-FS# clear spanning-tree detected-protocols
```

【Prompt Information】 -

【Platform Description】 -

5.5 clear spanning-tree mst topochange record

Clear the topology change information for the STP.

clear spanning-tree mst instance-id topochange record

【Parameter Description】

Parameter	Description
instance-id	The specified instance ID. For STP and RSTP protocols, only instance 0 is valid.

【Command Mode】 Privilege mode

【Default Level】 15

【Usage Guide】 Use this command to clear the topology change information for the specified instance.

【Configuration Example】 Clears the topology change information for the instance 0.

```
AC-FS# show spanning-tree mst 0 topochange record
Topology change information on mst 0:
 Time                Interface           Old status   New status   Type
 ------------------- ------------------- ------------ ------------ ----------------

 2013.5.1 4:18:46    GI0/6               Learning  Forwarding Normal
AC-FS# clear spanning-tree mst 0 topochange record
AC-FS# show spanning-tree mst 0 topochange record
%There's no topology change information has been record on mst 0.
```

【Prompt Information】 -

【Platform Description】 -

5.6 show spanning-tree

Displays and generates the global configuration information associated with the tree。

show spanning-tree [summary | forward-time | hello-time | max-age | inconsistentports | tx-hold-count | pathcost method | max-hops | counters]

【Parameter Description】

Parameter	Description
summary	Displays the information of each instance of MSTP and its port forwarding status.
forward-time	Display BridgeForwardDelay.
hello-time	Display BridgeHelloTime.
max-age	Display BridgeMaxAge.
inconsistentports	Displays ports blocked due to root protection or loop protection.
tx-hold-count	Displays the TxHoldCount.
pathcost method	Displays the method to calculate the path cost.
max-hops	Displays the maximum number of jumps for the instance.
counters	Displays the STP packet packet statistics.

【Command Mode】 Privilege mode, global mode, and interface mode

【Default Level】 15

【Usage Guide】 Use this command to view the global configuration information associated with the generation tree.

【Configuration Example】 1: View the BridgeHelloTime information of the spanning tree.

```
AC-FS# show spanning-tree hello-time
BridgeHelloTime :2
```

2: View the statistics of STP sending and receiving packets.

```
AC-FS# show spanning-tree counters

Port                              Receive      Send
GigabitEthernet 0/3               0            122594

MSTID      Port                              Receive      Send
0          GigabitEthernet 0/3               0            0
```

【Prompt Information】 -

【Platform Description】 -

5.7 show spanning-tree interface

View the STP transceiver packet statistics.

show spanning-tree interface interface-id [{ bpdufilter | portfast | bpduguard | link-type }]

【Parameter Description】

Parameter	Description
interface-id	The port number.
bpdufilter	Displays bpdufilter status.
portfast	Displays portfast status.
bpduguard	Display bpduguard status.
link-type	Display the linktype of the port

【Command Mode】 Privilege mode, global mode, and interface mode

【Default Level】 15

【Usage Guide】 Use this command to view the STP configuration information for the interface.

【Configuration Example】 View the STP configuration for the interface Gi 0 / 1.

```
AC-FS# show spanning-tree int gi 0/1

PortAdminPortFast : Disabled
PortOperPortFast : Disabled
PortAdminAutoEdge : Enabled
PortOperAutoEdge : Disabled
PortAdminLinkType : auto
PortOperLinkType : point-to-point
PortBPDUGuard : Disabled
PortBPDUFilter : Disabled
PortGuardmode  : None

###### MST 0 vlans mapped :ALL
PortState : forwarding
PortPriority : 128
PortDesignatedRoot : 32768.001a.a979.00ea
PortDesignatedCost  :  0
PortDesignatedBridge :32768.001a.a979.00ea
PortDesignatedPortPriority : 128
PortDesignatedPort : 1
PortForwardTransitions : 1
PortAdminPathCost  :  200000
PortOperPathCost : 200000
Inconsistent states : normal
PortRole : rootPort
```

【Field interpretation】

Field	Interpretation
Port Admin Port Fast	The Port Fast status of the port management configuration.
Port Oper Port Fast	The Port Fast status where the port is actually running.
Port Admin Auto Edge	The Auto Edge status of the port management configuration.
Port Oper Auto Edge	The Auto Edge status where the port is actually running.
Port Admin Link Type	The link type of the port management configuration.
Port Oper Link Type	The type of link that the port is actually running on.
Port BPDU Guard	Does the port BPDU Guard enable it.
Port BPDU Filter	Does the port BPDU Filter enable it.
Port Guard Mode	The Guard mode of the port.
Port State	Forward status of the port.

Port Priority	Port priority.
Port Designated Root	Assigned root bridge for the port.
Port Designated Cost	External root path overhead for the port.
Port Designated Bridge	Assigned network bridge for the port.
Port Designated Port Priority	The assigned port priority of the port.
Port Designated Port	Assigned port for the port.
Port Forward Transitions	Number of times that the ports change to the Forwarding status.
Port Admin Path Cost	Port management path overhead.
Port Oper Path Cost	Actual path overhead of the port.
Inconsistent states	Port root or loop inconsistent state.
Port Role	Port role.
Port Priority	Port priority.

【Prompt Information】 -

【Platform Description】 -

5.8 show spanning-tree mst

View the MST configuration, Instance for information.

show spanning-tree mst { configuration | instance-id [interface interface-id] }

【Parameter Description】

Parameter	Description
configuration	Device's mst configuration.
instance-id	Instance number.
interface-id	The port number.

【Command Mode】 Privilege mode, global mode, and interface mode

【Default Level】 15

【Usage Guide】 -

【Configuration Example】 View the information related to the resulting tree instance.

```
AC-FS# show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name      : test
Revision : 0
Instance  Vlans Mapped


0           : 2-4094
1           : 1
---------------------------------------------------------------------------------------------------------------
```

【Field interpretation】

Field	Interpretation
Multi spanning tree protocol	Can MSTP protocol.
Name	The name of the MST domain.
Revision	The version number of the MST domain.
Instance Vlans Mapped	Mapping relationship between the instance and the VLAN.

【Prompt Information】 -

【Platform Description】 -

5.9 show spanning-tree mst topochange record

View the record information for the resulting tree topology changes.

show spanning-tree mst instance-id topochange record

【Parameter Description】

Parameter	Description
instance-id	Instance ID.

【Command Mode】 Privilege mode, global mode, and interface mode

【Default Level】 15

【Usage Guide】 Use this command to view the topology changes of the port in the specified instance, which ports have changed in status, and why the status changes.

【Configuration Example】 View the record of the resulting tree topology change for instance 0.

```
AC-FS# show spanning-tree mst 0 topochange record
Topology change information on mst 0:
 Time                 Interface            Old status   New status   Type
 ___________________  ___________________  ___________  ___________  _______________

 2013.5.1 4:18:46     GI0/6                Learning     Forwarding   Normal
```

【Field interpretation】

Field	Interpretation
Time	Time of the topological changes in the interface
Interface	Interface where the topology changes occur
Old status	Interface of the old STP state
New status	Interface for a new STP state
Type	The reasons for the topological changes of the interface are divided into the following possible reasons： Normal --- Normal state changes of the interface, such as the interface UP / DOWN, the resulting state changes LoopGuard Block --- The interface enters due to ring inconsistency Block state RootGuard Block --- The interface is entered due to the root inconsistency Block state Inferior Block --- The interface enters the Block state by receiving a low-priority BPDU LoopGuard Unblock --- The interface recovers from the ring inconsistent state and enters the Forward state RootGuard Unblock --- The interface recovers from the root inconsistent state and enters the Forward state Inferior Unblock ---The interface does not receive a low priority again BPDU, goes into the Forward state

【Prompt Information】 If the specified instance is not topologically changed, then prompted below：

```
%There's no topology change information has been record on mst [ dec ].
where [ dec ] represents the instance ID.
```

【Platform Description】 -

【Parameter Description】 -

5.10 spanning-tree

Open the MSTP, and the parameters can set the basic settings for the MSTP global, while opening the MSTP.

spanning-tree [forward-time seconds | hello-time seconds | max-age seconds]

Turn off the spanning-tree function, if the no command with the parameter option simply restores the corresponding parameter to the default, but does not close the spanning tree.

no spanning-tree [forward-time | hello-time | max-age]

【Parameter Description】

Parameter	Description
forward-time seconds	The time interval for port status change, the value range is 4-30 seconds, and the default value is 15 seconds.
hello-time seconds	The interval at which the device regularly sends BPDUs. The value ranges from 1 to 10 seconds. The default value is 2 seconds.
max-age seconds	Maximum time for BPDU message message survival, with a value range of 6-40 seconds and a default value of 20 seconds.

【Default Configuration】 The spanning-tree default is closed.

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】 Forward-time, hello-time, max-age, the range of the three values is correlated, modifying one of which is affecting the range of the other two. There is a restriction relationship between these three values： 2*(Hello Time+1.0 seconds) <= Max-Age Time <= 2*(Forward-Delay–1.0 seconds). Values that do not meet this condition are also set as unsuccessful.

【Configuration Example】 1: Open the spanning-tree feature.

```
AC-FS(config)# spanning-tree
```

2： Set up the BridgeForwardDelay.

```
AC-FS(config)# spanning-tree  forward-time 10
```

【Verification】 1: Use the show running-config command to let you see if the command is set.

2: Use the show spanning-tree command to view the STP global configuration information.

【Prompt Information】 The STP protocol is mutually exclusive with the TRILL protocol of the data center. If you open the TRILL protocol first, and then open the STP protocol, it will be prompted as follows:

```
% Error! You must disable TRILL first.
```

【Common Mistake】 -

【Platform Description】 -

5.11 spanning-tree autoedge

Turn on the Autoedge switch for an interface.

spanning-tree autoedge

Turn off the Autoedge switch for an interface.

spanning-tree autoedge disabled

【Parameter Description】

Parameter	Description
disabled	Turn off the Autoedge switch for the interface.

【Default Configuration】 The default is open.

【Command Mode】 Interface mode

【Default Level】 15

【Usage Guide】 The assignment port is within a certain time range (3 seconds). If the BPDU from the downstream port is received, the port is connected to a network device, setting the port as the edge port and directly entering the Forwarding state. Ports automatically identified as edge ports are automatically identified as non-edge ports upon receipt of the BPDU. The edge port can be removed with the spanning-tree autoedge disabled command.

【Configuration Example】 Close the edge port automatic recognition switch of the interface Gi 1 / 1.

```
AC-FS(config)# interface gigabitethernet 1/1
AC-FS(config-if-interface-id-interface-id)# spanning-tree autoedge disabled
```

【Verification】 1. Use the show running-config command to let you see if the command is set.

2. Using the show spanning-tree interface command, you can view the STP configuration information for the interface.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.12 spanning-tree bpdufilter

Turn on the BPDU filter switch for an interface.

spanning-tree bpdufilter enabled

Turn off the BPDU filter switch for an interface.

spanning-tree bpdufilter disabled

【Parameter Description】

Parameter	Description
enabled	Turn on the BPDU filter switch of the interface.
disabled	Turn off the BPDU filter switch of the interface.

【Default Configuration】 The default is closed..

【Command Mode】 Interface configuration mode

【Default Level】 15

【Usage Guide】 When the BPDU Filter is opened, the corresponding port sends neither a BPDU nor receives the BPDU, and the port forwarding status is directly set to Forwarding.

【Configuration Example】 Turn on the BPDU Guard switch for the interface Gi 1 / 1.

```
AC-FS(config)# interface gigabitethernet 1/1
AC-FS(config-if-interface-id-interface-id)# spanning-tree bpdufilter enable
```

【Verification】 1: Use the show running-config command to let you see if the command is set.

2: Using the show spanning-tree interface command, you can view the STP configuration information for the interface.

【Prompt Information】 When the BPDU Guard feature takes effect, the following SYSLOG Prompt Information s are printed.

【Common Mistake】 -

【Platform Description】 -

5.13 spanning-tree bpduguard

Turn on the BPDU Guard switch for an interface。

spanning-tree bpduguard enabled

Turn off the BPDU Guard switch for an interface。

spanning-tree bpduguard disabled

【Parameter Description】

Parameter	Description
enabled	Turn on the BPDU Guard switch of the interface.
disabled	Turn off the BPDU Guard switch on the interface.

【Default Configuration】 The default is closed..

【Command Mode】 Interface configuration mode

【Default Level】 15

【Usage Guide】1. If the BPDU Guard of a single interface is opened, if the interface receives a BPDU, it enters the Error-disabled state.

2. Ports in the Error-disabled state that can be restored with the errdisable recovery [interval seconds].

【Configuration Example】 Turn on the BPDU Guard switch for the interface Gi 1 / 1.

```
AC-FS(config)# interface gigabitethernet 1/1
AC-FS(config-if-interface-id-interface-id)# spanning-tree bpduguard enable
```

【Verification】 1: Use the show running-config command to let you see if the command is set。

2: Using the show spanning-tree interface command, you can view the STP configuration information for the interface.

【Prompt Information】 When the BPDU Guard feature takes effect, the following SYSLOG Prompt Information s are printed. Where [char] indicates the port name.

```
SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port [ char ] with BPDU Guard enabled. Disabling port.
```

【Common Mistake】 -

【Platform Description】 -

5.14 spanning-tree compatible enable

Open the compatibility mode for the interface.

spanning-tree compatible enable

Turn off the compatibility mode of the interface.

no spanning-tree compatible enable

【Parameter Description】 -

【Default Configuration】 The default is the compatible mode that closes the interface..

【Command Mode】 Interface mode

【Default Level】 15

【Usage Guide】 1: Open the compatibility mode of the interface to send the MSTI information selectively according to the current port of the interface attributes information, so as to realize the interconnection with other manufacturers. Examples are as follows:

//Create an instance of 1,2.

spanning-tree mst configuration instance 1 vlan 1

instance 2 vlan 2

If interface 1 only belongs to VLAN 1, enable the STP compatibility mode of the interface, and the BPDU sent by interface 1 only carries instance 0 and instance 1, and does not carry the information of instance 2.

2: Opening the compatibility mode of the interface, the STP calculates whether the interface participates in the calculation of the specified instance based on the VLAN where the interface belongs, and the mapping relationship of the VLAN and the instance.

3: Opening the compatibility mode of the interface, the STP calculates whether the interface participates in the calculation of the specified instance based on the VLAN where the interface belongs, and the mapping relationship of the VLAN and the instance.

【Configuration Example】 Open the interface-compatible mode for the interface Gi 0 / 1.

```
AC-FS(config)# interface gigabitethernet 0/1
AC-FS(config-if-interface-id-interface-id)#spanning-tree compatible enable
```

【Verification】 Use the show running-config command to let you see if the command is set.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.15 spanning-tree guard loop

Open the loop guard feature on the interface.

spanning-tree guard loop

Turn off the loop guard feature on the interface.

no spanning-tree guard loop

【Parameter Description】 -

【Default Configuration】 The loop guard feature is turned off by default..

【Command Mode】 Interface configuration mode

【Default Level】 15

【Usage Guide】 1. Enabling loop guard prevents possible loops from the root or backup port from failing to receive bpdu .

2. The loop guard and root guard features on the interface are mutually exclusive.

【Configuration Example】 Open the Loop Guard function of the interface Gi 0 / 1.

```
AC-FS(config)# interface gigabitethernet 0/1
AC-FS(config-if-interface-id)# spanning-tree guard loop
```

【Verification】 Use the show running-config command to let you see if the command is set.

【Prompt Information】 The loop guard and root guard functions of the interface are mutually exclusive. When root guard is configured first before loop guard, this is prompted below SYSLOG:

SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Root Guard disabled on port [chars].

Where [chars] represents the interface name.

【Common Mistake】 -

【Platform Description】 -

5.16 spanning-tree guard none

Turn off the guard feature on the interface.

spanning-tree guard none

Undo the interface, guard, function off.

no spanning-tree guard none

【Parameter Description】 -

【Default Configuration】 The guard feature is turned off by default

.

【Command Mode】 Interface configuration mode

【Default Level】 15

【Usage Guide】 -

【Configuration Example】 Turn off the guard feature of the interface, Gi 0 / 1.

```
AC-FS(config)# interface gigabitethernet 0/1
AC-FS(config-if-interface-id)# spanning-tree guard none
```

【Verification】 Use the show running-config command to let you see if the command is set

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.17 spanning-tree guard root

Open the root guard feature for an interface.

spanning-tree guard root

Turn off the root guard feature of an interface.

【Parameter Description】 -

【Default Configuration】 The root guard feature is turned off by default

【Command Mode】 Interface configuration mode

【Default Level】 15

【Usage Guide】 Table 1. Enables root guard to prevent changes in the current root bridge status due to misconfiguration or attacks on illegal messages.

Table 2. The root guard and loop guard functions of the interface are mutually exclusive.

【Configuration Example】 Open the root guard feature of the interface Gi 0 / 1.

```
AC-FS(config)# interface gigabitethernet 0/1
AC-FS(config-if-interface-id)# spanning-tree guard root
```

【Verification】 Use the show running-config command to let you see if the command is set.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.18 spanning-tree ignore tc

Turn on the tc filter switch for an interface.

spanning-tree ignore tc

Turn off the tc filter switch for an interface.

no spanning-tree ignore tc

【Parameter Description】 -

【Default Configuration】 The TC filtering function is turned off by default.

【Command Mode】 Interface mode

【Default Level】 15

【Usage Guide】 With tc filtering enabled, the TC messages received by the port are not processed.

【Configuration Example】 Open the TC filter for the interface Gi 0 / 1.

```
AC-FS(config)# interface gigabitethernet 0/1
AC-FS(config-if-interface-id)# spanning-tree ignore tc
```

【Verification】 Use the show running-config command to let you see if the command is set.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.19 spanning-tree link-type

Configure the connection type for the interface.

spanning-tree link-type [point-to-point | shared]

The connection type for the recovery interface is the default value.

no spanning-tree link-type

【Parameter Description】

Parameter	Description
poinit-to-point	Force the connection type of this interface to be point-to-point.
shared	Force the connection type of the interface to shared.

【Default Configuration】 When the interface type is full-duplex, the connection type of the interface is point-to-point; the interface connection type is shared when the interface type is half-duplex.

【Command Mode】 Interface configuration mode

【Default Level】 15

【Usage Guide】 Configuring whether the connection type of the port is a "point-to-peer connection" concerns whether RSTP can converge quickly. When the user does not set the value, the device automatically sets on the duplex status of the port.

【Configuration Example】 The connection type for the configuration interface Gi 1 / 1 is point-to-point.

```
AC-FS(config)# interface gigabitethernet 1/1
AC-FS(config-if-interface-id)# spanning-tree link-type point-to-point
```

【Verification】 1: Use the show running-config command to let you see if the command is set.

2: Use the show spanning-tree interface command to view the STP interface configuration.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.20 spanning-tree loopguard default

Open on the global loop guard properties.

spanning-tree loopguard default

Turn off the global loop guard properties.

no spanning-tree loopguard default

【Parameter Description】 -

【Default Configuration】 The loop guard feature is turned off by default.

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】Enabling loop guard prevents possible loops from the root or backup port from failing to receive bpdu.

【Configuration Example】 Open the loop guard property.

```
AC-FS(config)# spanning-tree loopguard default
```

【Verification】 Use the show running-config command to let you see if the command is set.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】

5.21 spanning-tree max-hops

Sets the maximum number of jumps for the BPDU frame.

spanning-tree max-hops hop-count

Restore to default value.

no spanning-tree max-hops

【Parameter Description】

Parameter	Description
hop-count	The number of times a BPDU can pass through the device before being discarded, in the range 1-40.

【Default Configuration】 The default value of the hop-count is 20.

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】 Within Region, the BPDU sent by Root Bridge contains a Hot Count item. Starting with Root Bridge, Hop Count decreases 1 for each device until 0 indicates that the BPDU information timeout and the device drops the BPDU with a Hops value of 0. This command specifies how many devices the BPDU passes discarded within a Region. Changing the max-hops will affect all the Instance.

【Configuration Example】 The next example will set the Max-hops value for all MST Instance s to 10:

```
AC-FS(config)# spanning-tree max-hops 10
```

【Verification】 Use the show running-config command to let you see if the command is set.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.22 spanning-tree mode

Configure the generation tree mode.

spanning-tree mode [stp | rstp | mstp]

Restore the generated tree mode to the default value.

no spanning-tree mode

【Parameter Description】

Parameter	Description
Stp	Spanning tree protocol (IEEE 802.1d).
Rstp	Rapid spanning tree protocol (IEEE 802.1w).
Mstp	Multiple spanning tree protocol (IEEE 802.1s).

【Default Configuration】 MSTP version.

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】 Some friendly business products are not fully implemented according to the standards, which may lead to some compatibility problems. Use this command to switch to a lower version of Spanning Tree mode for compatibility when the administrator finds that it is not compatible with this device.

When switching from MSTP mode to RSTP or STP mode, all information about MSTP Region will be cleared.

Switching the spanning tree mode will cause the spanning tree to be recalculated.

【Configuration Example】 Configure the generation tree in STP mode.

```
AC-FS(config)# spanning-tree mode stp
```

【Verification】 1: Use the show running-config command to let you see if the command is set.

2: Use the show spanning-tree command to view the spanning tree configuration.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.23 spanning-tree mst configuration

Configure the MSTP Region, and go into MST mode.

spanning-tree mst configuration

Restore all the parameters in MST mode to the default value.

no spanning-tree mst configuration

【Parameter Description】 -

【Default Configuration】 The default instance and vlan correspondence is that all Vlan are in Instance 0 . The name is an empty string. The revision is 0

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】 To return to privileged mode, enter the end command, or type the Ctrl + C combo key. To return to the global configuration mode, enter the exit command. When you enter MST configuration mode, you can use the following command for the configuration parameters:

For FS devices with small physical memory (such as 64M memory), creating 64 instance s under stacking will cause insufficient memory. It is recommended that you control the number of instance s created when stacking.

For FS devices with small physical memory (such as 64M memory), creating 64 instance s under stacking will cause insufficient memory. It is recommended that you control the number of instance s created when stacking.

For FS devices with small physical memory (such as 64M memory), creating 64 instance s under stacking will cause insufficient memory. It is recommended that you control the number of instance s created when stacking.

【Configuration Example】 1. An example below shows how to enter the MST mode, mapping VLAN 3,5-10 to

```
AC-FS(config)# spanning-tree mst configuration
AC-FS(config-mst)# instance 1 vlan 3, 5-10 AC-
FS(config-mst)# name region1
AC-FS(config-mst)# revision 1
AC-FS(config-mst)# show spanning-tree mst configuration
MST configuration
Name [region1]
Revision 1
Instance  Vlans Mapped
```

```
0           1-2,4,11-4094
1           3,5-10
```

```
AC-FS(config-mst)# exit AC-FS(config)#
```

2: If you want to remove VLAN 3 from Instance 1, after entering MST configuration mode, perform the following procedure:

```
AC-FS(config-mst)# no instance 1 vlan 3
```

3: If you want to delete the entire Instance 1, this is as follows:

```
AC-FS(config-mst)# no instance 1
```

【Verification】 Use the show running-config command to let you see if the command is set.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.24 instance instance-id vlan-range

Set the instances and vlan mapping relationships in MST configuration mode.

instance instance-id vlan vlan-range

All the instance configuration returns to the default value in MST configuration mode.

no instance instance-id {vlan vlan-range}

【Parameter Description】

Parameter	Description
instance-id	Instance number, the range is 0-64.
vlan-range	List of Vlans, range 1 – 4094.

【Default Configuration】 The default instance and vlan correspondence is that all Vlan are in Instance 0 .

【Command Mode】 MST Config mode

【Default Level】 15

【Usage Guide】 After entering the MST configuration mode, use the following command for the configuration parameters:

instance instance-id vlan vlan-range: Add the Vlan group to the MST Instance. Here the range of the instance-id is 0-64. The range of vlan is 1-4094. The vlan-range can be a collection of vlan, separated by commas, and continuous VLAN ID s can connect the head and end of two VLAN ID s, for example: instance 10 vlan 2,3,6-9 defines adding VLAN 2,3,6,7,8,9 to the Instance 10. The default configuration is that all VLAN are in Instance 0. The way to remove a VLAN from the Instance is by using the no command: no instance instance-id [vlan vlan-range].(Note that the Instance range in the no command is 1-64). For FS devices with small physical memory (such as 64M memory), creating 64 instance s under stacking will cause insufficient memory. It is recommended that you control the number of instance s created when stacking.

【Configuration Example】 1. An example below shows how to enter the MST mode, mapping VLAN 3,5-10 to MST Instance 1.

```
AC-FS(config)# spanning-tree mst configuration AC-FS(config-mst)#
instance 1 vlan 3， 5-10 AC-FS(config-mst)# show spanning-tree mst
configuration
Multi spanning tree protocol : Enable
Name :
Revision : 0
Instance Vlans Mapped

0 1-2,4,11-4094
1 3,5-10
AC-FS(config-mst)# exit AC-FS(config)#
```

2: If you want to remove VLAN 3 from Instance 1, after entering MST configuration mode, perform the following procedure.

```
AC-FS(config-mst)# no instance 1 vlan 3
```

3: If you want to delete the entire Instance 1, this is as follows:

```
AC-FS(config-mst)# no instance 1
```

【Verification】 Use the show running-config command to let you see if the command is set.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.25 revision

Set the revision value of the MSTP field in MST configuration mode,

revision version

In MST configuration mode, all instance configurations are restored to default values.

no revision

【Parameter Description】

Parameter	Description
version	Specify the MST revision number in the range 0-65535.

【Default Configuration】 The default revision is 0 .

【Command Mode】 MST Config mode

【Default Level】 15

【Usage Guide】 After entering the MST configuration mode, you can use the following command for the configuration parameters: revision version: Set the number of MST versions, range 0-65535. You can restore it to the default value with the no revision .show spanning-tree mst configuration: Displays the current MST region information.

【Configuration Example】 The following example shows how to enter MST mode and configure revision to 1.

```
AC-FS(config)# spanning-tree mst configuration AC-FS(config-mst)# revision 1.
AC-FS(config)#       spanning-tree       mst       configuration
AC-FS(config-mst)# revision 1
AC-FS(config-mst)#    show    spanning-tree    mst    configuration    Multi
spanning tree protocol : Enable
Name          : Revision :
1
Instance   Vlans Mapped


 0               : ALL
```

```
AC-FS(config-mst)# exit
AC-FS(config)#
```

【Verification】 Use the show running-config command to let you see if the command is set

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.26 name

Modify the MST configuration name in MST configuration mode.

name name

Return the MST configuration name to the default value in MST configuration mode.

no name

【Parameter Description】

Parameter	Description
name	MST name configuration, the string can have up to 32 bytes.

【Default Configuration】 The default name is an empty string.

【Command Mode】 MST Config mode

【Default Level】 15

【Usage Guide】 After entering the MST configuration mode, you can use the following command for the configuration parameters: name name Specifies the MST configuration name that can contain up to 32-character strings.

You can restore it to the default value with the no name. Show spanning-tree mst configuration: Displays the current MST region information.

【Configuration Example】 The following example shows how to enter MST mode, configure revision to 1.

```
AC-FS(config)#       spanning-tree       mst       configuration
AC-FS(config-mst)# name region1
AC-FS(config-mst)#   show   spanning-tree   mst   configuration   Multi
spanning tree protocol : Enable
Name         : region1 Revision : 0
Instance   Vlans Mapped


0                : ALL
```

```
AC-FS(config-mst)# exit
AC-FS(config)#
```

【Verification】 Use the show running-config command to let you see if the command is set.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.27 spanning-tree mst cost

Set the path cost per Instance in interface mode.

spanning-tree [mst instance-id] cost cost

Restore the Instance path cost of an interface to the default value.

no spanning-tree [mst instance-id] cost

【Parameter Description】

Parameter	Description
instance-id	Instance number, the range is 0-64.
cost	Path cost value, in the range 1-200,000,000.

【Default Configuration】 The default value for the Instance-ID is 0.

The default value is automatically calculated based on the link rate of the Interface.

1000 Mbps—20000

100 Mbps—200000

10 Mbps—2000000

【Command Mode】 Interface configuration mode

【Default Level】 15

【Usage Guide】 Larger cost value indicates a higher path cost.

【Configuration Example】 The configuration path cost value for an interface associated with Instance 3 is 400 is as follows:

```
AC-FS(config)# interface gigabitethernet 1/1
AC-FS(config-if-interface-id)# spanning-tree mst 3 cost 400
```

【Verification】 1: Use the show running-config command to let you see if the command is set.

2: Using the show spanning-tree mst interface interface-id command, you can verify the above configuration.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.28 spanning-tree mst port-priority

Set an interface with a different port priority for different Instance s。

spanning-tree [mst instance-id] port-priority priority

Restore the Instance for an interface to the default value。

no spanning-tree [mst instance-id] port-priority

【Parameter Description】

Parameter	Description
Instance-id	Instance number, the range is 0-64
priority	Port priority, optional 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240, a total of 16 integers, all multiples of 16.

【Default Configuration】 The default value for the Instance-id is 0,The default value for the priority is 128

【Command Mode】 Interface configuration mode.

【Default Level】 15

【Usage Guide】 When loop ops within Region, high priority ports are in the send state. With the same priority, select a port with smaller slogans. Using this command, this affects which port in the forming loop within the Region is in the sending state.

【Configuration Example】 The next example sets the priority value of the Gigabitethernet 1 / 1 interface in the Instance 20 to 0:

```
AC-FS(config)# interface gigabitethernet 1/1
AC-FS(config-if-interface-id)# spanning-tree mst 20 port-priority 0
```

【Verification】 1: Use the show running-config command to let you see if the command is set.
2: Using the show spanning-tree mst interface interface-id command, you can verify the above configuration.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.29 spanning-tree mst priority

Set the device priority for the Instance.

spanning-tree [mst instance-id] priority priority

Set the device priority for the Instance to recover to the default value.

no spanning-tree [mst instance-id] priority

【Parameter Description】

Parameter	Description
instance-id	Instance number, the range is 0-64.
priority	Device priority, optional 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 and 61440. There are 16

	integers in total, all of which are multiples of 4096.

【Default Configuration】 The default value for instance-id is 0 and priority is 32768.

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】 Setting the device priority concerns which device is the root of the entire network, and also concerns the topology of the entire network.

【Configuration Example】 The following example sets the device priority value for the Instance 20 to 8192:

```
AC-FS(config)# spanning-tree mst 20 priority 8192
```

【Verification】 1. Use the show running-config command to let you see if the command is set.

2. Use the show spanning-tree command to verify the above configuration.

【Prompt Information】 The set bridge priority is not a multiple of 4096 and will prompt the following information:

bridge priority must be IN increments of 4096.

【Common Mistake】 -

【Platform Description】 -

5.30 spanning-tree pathcost method

Configure the port path cost.

spanning-tree pathcost method { long [standard] | short }

The cost of restoring the port path is calculated by default.

no spanning-tree pathcost method

【Parameter Description】

Parameter	Description

long [standard]	Use the 802.1t standard to set the value of path-cost. standard means to calculate the cost value according to the formula recommended by the standard.
short	Use the 802.1d standard to set the value of path-cost.

【Default Configuration】 The value of the 802.1T standard sets the Path-cost by default.

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】 When the port Path Cost is the default value, the device automatically calculates the port's Path Cost based on the port rate.

By default, our company's private long integer mode is adopted. After the path cost scheme of the standard recommended scheme is modified, the cost of the AP will change with the number of UP member ports, and the change of the port cost will cause the network topology to change.

【Configuration Example】 The cost of configuring the port path is calculated as long：

```
AC-FS(config)# spanning-tree pathcost method long
```

【Verification】 1: Use the show running-config command to let you see if the command is set.

2: Use the show spanning-tree command to see if the command is configured.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.31 spanning-tree portfast

Turn on the Portfast switch for an interface.

spanning-tree portfast

Turn off the Portfast switch for an interface.

spanning-tree portfast disabled

【Parameter Description】

Parameter	Description
disabled	Turn off the Portfast switch on the interface.

【Default Configuration】 The default is closed.

【Command Mode】 Interface configuration mode

【Default Level】 15

【Usage Guide】 On Port Fast, the port will directly Forwarding. But then the Port Fast Operational State is made to be because you receive the BPDU disabled, and thus normally participating in the STP calculation.

【Configuration Example】 Turn on the Portfast switch for the interface Gi 1 / 1:

```
AC-FS(config)# interface gigabitethernet 1/1
AC-FS(config-if-interface-id)# spanning-tree portfast
```

【Verification】 1: Use the show running-config command to let you see if the command is set.

2: Use the show spanning-tree interface command to see if the command is configured.

【Prompt Information】 Open the Port Fast switch of the interface and prompt the following information:

```
%Warning: portfast should only be enabled on ports connected to a single host. Connecting hubs,
switches, bridges to this interface when portfast is enabled,can cause temporary loops.
```

【Common Mistake】 -

【Platform Description】 -

5.32 spanning-tree portfast bpdufilter default

Turn on the global BPDU filter switch.

spanning-tree portfast bpdufilter default

Turn off the global BPDU filter s.

no spanning-tree portfast bpdufilter default

【Parameter Description】 -

【Default Configuration】 Close the BPDU filter by default..

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】 1. The global BPDU Filter is combined with the port's Port Fast feature to take effect.

2. When the global BPDU Filter is opened and the port is the Port Fast port, the port neither issues nor receives a BPDU. Use the show spanning-tree command to view the settings.

【Configuration Example】 Turn on the Portfast switch for the interface Gi 1 / 1:

```
AC-FS(config)# spanning-tree portfast bpdufilter default
```

【Verification】1: Use the show running-config command to let you see if the command is set.

2: Use the show spanning-tree interface command to see if the command is configured.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.33 spanning-tree portfast bpduguard default

Open the global BPDU guard.

spanning-tree portfast bpduguard default

Turn off the global BPDU guards.

no spanning-tree portfast bpduguard default

【Parameter Description】 -

【Default Configuration】 Close the global BPDU Guard s by default.

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】 Open BPDU guard and if you receive B r r D U on that port, error-disabled status. Use the show spanning-tree The command views the settings.

When portfast is enabled on an interface, the global BPDU guard configuration takes effect.

【Configuration Example】 Open the BPDU Guard:

```
AC-FS(config)# spanning-tree portfast bpduguard default
```

【Verification】 1: Use the show running-config command to let you see if the command is set.

2: Use the show spanning-tree command to see if the command is configured.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.34 spanning-tree portfast default

Open the Portfast switch for all of the interfaces.

spanning-tree portfast default

Close the Portfast switch for all interfaces.

no spanning-tree portfast default

【Parameter Description】 -

【Default Configuration】 Close the Portfast switch for all interfaces by default.

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】 -

【Configuration Example】 Open the Portfast switch for all of the interfaces:

```
AC-FS(config)# spanning-tree portfast default
```

【Verification】 Use the show running-config command to let you see if the command is set.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.35 spanning-tree reset

Restore the entire spanning-tree settings to the default value.

spanning-tree reset

【Parameter Description】-

【Default Configuration】 -

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】1: Global configuration mode.

2: Configure the spanning-tree reset command to default for the build tree protocol switch status. When the STP protocol is open, configure the spanning-tree reset command and the STP protocol is still open.

【Configuration Example】 Restore the entire generation tree configuration to the default value:

```
AC-FS(config)# spanning-tree reset
```

【Verification】 Use the show running-config command to see if the STP command is restored to the default value.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.36 spanning-tree tc-guard

Turn on the tc-guard switch for an interface.

spanning-tree tc-guard

Turn off the tc-guard switch for an interface.

no spanning-tree tc-guard

【Parameter Description】 -

【Default Configuration】 Turn off the tc-guard switch off by default.

【Command Mode】 Interface configuration mode

【Default Level】 15

【Usage Guide】 Enable the tc-guard function to prevent the spread of tc messages.

【Configuration Example】 Open the tc-guard switch for the interface Gi 1 / 1:

```
AC-FS(config)# interface gigabitethernet 1/1
AC-FS(config-if-interface-id)# spanning-tree tc-guard
```

【Verification】 Use the show running-config command to let you see if the command is set.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.37 spanning-tree tc-protection

Turn on the tc-protection switch.

spanning-tree tc-protection

Turn on the tc-protection switch.

no spanning-tree tc-protection

【Parameter Description】 -

【Default Configuration】 Turn off the tc-protection switch off by default.

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】 -

【Configuration Example】 Turn on the tc-protection switch:

```
AC-FS(config)# spanning-tree tc- protection
```

【Verification】 Use the show running-config command to let you see if the command is set.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.38 spanning-tree tc-protection tc-guard

Turn on the global tc-guard switch.

spanning-tree tc-protection tc-guard

Global close the tc-guard switch.

no spanning-tree tc-protection tc-guard

【Parameter Description】 -

【Default Configuration】 The global tc-guard switch is closed by default

.

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】Enable the tc-guard function to prevent the spread of tc messages.

【Configuration Example】 Turn on the tc-guard switch:

```
AC-FS(config)# spanning-tree tc-protection tc-guard
```

【Verification】 Use the show running-config command to let you see if the command is set.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.39 spanning-tree tx-hold-count

Configure TxHoldCount, the maximum number of BPDU sent per second.

spanning-tree tx-hold-count tx-hold-count

Configure the TxHoldCount to recover to the default value。

no spanning-tree tx-hold-count

【Parameter Description】

Parameter	Description
tx-hold-count	TxHoldCount setting. The value range is 1-10, and the default value is 3.

【Default Configuration】 The default value is 3.

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】-

【Configuration Example】 Global configuration mode:

```
AC-FS(config)# spanning-tree tx-hold-count 5
```

【Verification】 Use the show running-config command to let you see if the command is set.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】

6 MAC VLAN

6.1 mac-vlan enable

Open the MAC VLAN feature on the port.

mac-vlan enable

Turn off the MAC VLAN feature on the port.

no mac-vlan enable

Restore the MAC VLAN functionality on the port.

default mac-vlan enable

【Parameter Description】 -

【Default Configuration】 The MAC VLAN function on the port is turned off.

【Command Mode】 Interface mode

【Default Level】 15

【Usage Guide】 After the MAC VLAN switch must be turned on the port for the globally configured MAC VLAN table item to take effect on the port. MAC VLAN is only enabled on hybrid ports, not on other ports.

【Configuration Example】 Open the MAC VLAN feature on the port:

```
AC-FS(config-if-interface-id)# mac-vlan enable
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

6.2 mac-vlan mac-address

Configure the static MAC VLAN table items.

mac-vlan mac-address mac-address [mask mac-mask] vlan vlan-id [priority pri_val]

Remove the static MAC VLAN table item.

no mac-vlan mac-address mac-address [mask mac-mask] vlan vlan-id [priority pri_val]

Remove the static MAC VLAN table item.

default mac-vlan mac-address mac-address [mask mac-mask] vlan vlan-id [priority pri_val]

【Parameter Description】

Parameter	Description
mac-address	Specify the MAC address.
mac-mask	Specify MAC address mask, high must be 1 in binary. The field is set by default to full F.
vlan-id	Specify the VLAN corresponding to the MAC address with a value of 1 to 4094.
pri_val	Specifies the 802.1p priority of the VLAN corresponding to the MAC address. The value is 0 ~ 7, and the default value is 0.

【Default Configuration】 The static MAC VLAN table item is not configured by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 The mac-vlan mac-address command is used to configure the VLAN for the MAC address and its priority. The no mac-vlan command is used to remove the MAC address association with the VLAN.

【Configuration Example】 Configure the static MAC VLAN table items:

```
AC-FS(config)# mac-vlan mac-address 0001.0001.0001 vlan 100 priority 3
AC-FS(config)# mac-vlan mac-address 0002.0002.0000 mask ffff.ffff.0000 vlan 200 priority 5
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

6.3 show mac-vlan

View the MAC VLAN table item.

show mac-vlan { all | dynamic | static | vlan vlan-id | mac-address mac-address [mask mac-mask] }

【Parameter Description】

Parameter	Description
all	Displays all of the table items for the MAC-VLAN table.
dynamic	Displays the dynamically configured MAC-VLAN table items.
static	Displays the MAC-VLAN table items for the static configuration.
vlan vlan-id	Displays the MAC-VLAN table item for the specified VLAN.
mac-address mac-address	The MAC-VLAN table items are displayed ON by MAC.
mask mac-mask	Displays the MAC-VLAN table item for the specified MAC address range.

【Command Mode】 All mode

【Default Level】 2

【Usage Guide】 When you specify a mac-address parameter, but the mask parameter is not specified, the MAC-VLAN table item for a single MAC address is displayed. When you specify both the mac-address and mask parameters, you display the MAC VLAN table items that specify the MAC address range.

【Configuration Example】 Displays all of the MAC-VLAN table items:

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

6.4 show mac-vlan interface

View the list of ports that turn the MAC VLAN feature on

show mac-vlan interface

【Parameter Description】 -

【Command Mode】 All mode

【Default Level】 2

【Usage Guide】 With MAC VLAN turned on the port, use this command to confirm that the configuration is successful.

【Configuration Example】 View the MAC address table:

```
AC-FS# show mac-vlan interface
MAC VLAN is enabled on following interface:
------------------------------------------

FastEthernet 0/3
FastEthernet 0/10
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】

7 VLAN-Group

7.1 vlan-assign-mode

On an AC device, configure the VLAN assignment mode for the current VLAN-Group s or all VLAN-Groups.

Configure the VLAN assignment mode

vlan-assign-mode {dot1x | mac-hash}

Unconfiguration, VLAN, allocation mode.

no vlan-assign-mode

【Parameter Description】

Parameter	Description
dot1x	After the 802.1x authentication is successful, the authentication server issues the VLAN to the user.
mac-hash	VLAN assignment for the user terminal according to the MAC address hash case.

【Default Configuration】 The assignment pattern of VLAN-Group is none.

【Command Mode】 VLAN-Group configuration mode, or global configuration mode

【Default Level】 14

【Usage Guide】 If configured in global configuration mode, effective for all VLAN-Group. If configured in VLAN-Group configuration mode, effective only for the current VLAN-Group. Based on VLAN-Group configuration, priority over global configuration.
VLAN distribution mode can be based on 802.1x VLAN distribution or VLAN distribution for user terminal based on MAC address and VLAN distribution for user terminal. At present, VLAN distribution according to the idle status of DHCP server address pool is not supported.

【Configuration Example】 The VLAN assignment mode for configuring the VLAN-Group 10 is in the dot1x mode:

```
AC-FS(config)# vlan-group 10
AC-FS(config-vlan-group)# vlan-assign-mode dot1x
```

【Verification】 show vlan-group 10 View the configuration information for the vlan allocation mode.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

7.2 vlan-group

Create VLAN-Group.

vlan-group group-id

Delete VLAN-Group.

no vlan-group group-id

【Parameter Description】

Parameter	Description
group-id	VLAN-Group ID, range <1-128>.

【Default Configuration】 -

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】None

【Configuration Example】 On an AC device, create a VLAN-Group 100:

```
AC-FS# configure terminal AC-FS(config)#
vlan-group 100
AC-FS(config-vlan-group)#
```

【Verification】 Show vlan-group See if the VLAN-Group 100 is configured.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

7.3 default-vlan

Configure the default VLAN for the VLAN-Group.

default-vlan vlan-id

Cancel the default VLAN for the VLAN-Group.

no default-vlan vlan-id

【Parameter Description】

Parameter	Description
vlan-id	The VLAN-ID is the VLAN within the VLAN set of the VLAN-Group.

【Default Configuration】 Default VLAN is not specified by default.

【Command Mode】 VLAN-Group configuration mode

【Default Level】 14

【Usage Guide】When you configure the default-assigned VLAN, you must first add the VLAN to the corresponding VLAN-Group. The default VLAN value works only when the authentication server performs a VLAN issue to the VLAN user after the VLAN allocation mode of the current WLAN is 802.1x authentication.

【Configuration Example】 The default VLAN for the VLAN-Group 100 is 10.

```
AC-FS# configure terminal AC-FS(config)#
vlan-group 100
AC-FS(config-vlan-group)# default-vlan 10
```

【Verification】 show vlan-group 100 View the default vlan configuration information.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

7.4 vlan-list

On an AC device, configure the list of VLAN members that the specified VLAN-Group contains.The command is as follows：

vlan-list vlan-list

Cancel the vlan-list.

no vlan-list

【Parameter Description】

Parameter	Description
vlan-list	VLAN list, and the maximum number of members is 128.

【Default Configuration】 The vlan-list default is not configured.

【Command Mode】 VLAN-Group configuration mode

【Default Level】 14

【Usage Guide】 If a WLAN needs to map multiple VLAN, multiple VLAN are added to the same VLAN-Group, and then VLAN-Group is associated with WLAN.

【Configuration Example】 On the AC device, the VLAN 100-105 was added to the VLAN-Group 100.

```
AC-FS# configure terminal AC-FS(config)#
vlan-group 100
AC-FS(config-vlan-group)# vlan-list 100-105
AC-FS(config-vlan-group)# default-vlan 10
```

【Verification】 show vlan-group 100 View the vlan list configuration information.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

7.5 vlan-group

Configure the VLAN-Group for the association and WLAN association

vlan-group group-id

【Parameter Description】

Parameter	Description
group-id	VLAN-Group ID，range <1-128>.

【Default Configuration】 No VLAN-Group is associated by default.

【Command Mode】 WLAN configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】 -

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

7.6 show vlan-group

On the AC device, the VLAN-Group information is displayed with the following command：

show vlan-group [group-id]

【Parameter Description】

Parameter	Description
group-id	VLAN-Group ID.

【Command Mode】 Privilege mode

【Default Level】 2

【Usage Guide】 -

【Configuration Example】 On the AC device, display the VLAN member information for all the VLAN-Group.

```
AC-FS# show vlan-group
VLAN-Group ID    Default VLAN   Assign-Mode        VLAN-List
_____________    ____________   ________________   ____________________________
128          NA          dot1x          110-130，141-150
```

【Prompt Information】 -

【Platform Description】

8 PPP

8.1 ppp accm

Configure ACCM (Asynchronous Character Conversion Mask) option for PPP negotiation.

ppp accm value

Restore Defaults.

no ppp accm

【Parameter Description】

Parameter	Description
value	Value of the ACCM option, in the range from 0 to 0xffffffff.

【Command Mode】 Interface configuration mode

【Default Configuration】 The default is 0x000A0000.

【Default Level】 14

【Usage Guide】This command is used to configure the ACCM option involved in the PPP negotiation phase, in the range from 0 to 0xffffffff. The default is 0x000A0000.

【Configuration Example】 The following example configures the ACCM option for PPP negotiation.

```
AC-FS(config-if-Virtual-ppp 1)#ppp accm 0x0000000f
AC-FS(config-if-Virtual-ppp 1)#
```

【Verification】 Run the show running-config command to display the value of the ACCM option configured on the current interface for PPP negotiation.

【Prompt Information】 -

【Platform Description】 -

8.2 ppp accounting

Configure the accounting method of PPP.

ppp accounting { default | list_name }

Delete PPP's billing list.

no ppp accounting

【Parameter Description】

Parameter	Description
default	Default accounting list.
list_name	Name of the AAA accounting list.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 This command is used to configure the accounting mode of PPP. You can set the accounting mode to the default list or to the name of a specified accounting list. Before configuring this command, you need to enable the AAA module; otherwise, this command is invisible.

【Configuration Example】 The following example configures the accounting mode of PPP.

```
  AC-FS#conf
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)#aaa new-model
AC-FS(config)#int virtual-ppp 1
AC-FS(config-if-Virtual-ppp 1)#ppp accounting default
AC-FS(config-if-Virtual-ppp 1)#
```

【Verification】 Run the show running-config command to display the name of the PPP accounting list configured on the current interface.

【Prompt Information】 -

【Platform Description】 -

8.3 ppp authentication

Configure the PPP authentication method.

ppp authentication { { pap | chap | ms-chap | ms-chap-v2 } [callin | { chap | pap } | default | list_name] }

Delete the authentication method of PPP

no ppp authentication { { pap | chap | ms-chap | ms-chap-v2 } [callin | { chap | pap } | default |

list_name] }

【Parameter Description】

Parameter	Description
pap	Configure the authentication method as PAP.
callin	Only authenticate incoming request packets.
chap	Configure the authentication method as CHAP.
default	Whether it is PAP or CHAP authentication, use the default authentication list.
list_name	Authentication list name when configuring authentication.
ms-chap	Configure the authentication method as ms-chap.
ms-chap-v2	Configure the authentication method as ms-chap-v2.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 This command is used to configure the authentication mode of PPP, which may be PAP or CHAP authentication.

【Configuration Example】 The following example configures the authentication mode of PPP.

```
AC-FS(config-if-Virtual-ppp 1)#ppp authentication pap
AC-FS(config-if-Virtual-ppp 1)#ppp authentication chap
AC-FS(config-if-Virtual-ppp 1)#ppp authentication pap chap callin default
AC-FS(config-if-Virtual-ppp 1)#ppp authentication pap chap test_list
AC-FS(config-if-Virtual-ppp 1)#
```

【Verification】 Run the show running-config command to display whether the authentication mode of PPP has been configured on the current interface.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

8.4 ppp authorization

Use this command to configure the authorization list of AAA authentication of PPP.

ppp authorization { default | list_name}

Use this command to delete the authorization list of AAA authentication of PPP.

no ppp authorization

【Parameter Description】

Parameter	Description
default	Default authorization list of AAA authentication of PPP.
list_name	Name of the specified authorization list of AAA authentication of PPP.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 This command is used to configure the authorization list of AAA authentication of PPP. The authorization list of AAA authentication is used in the PPP authentication phase to perform AAA authentication. This command is visible only after the AAA module is enabled.

【Configuration Example】 The following example sets the authorization list of PPP authentication on interface Virtual-PPP 1 to auth_list.

```
  AC-FS(config)#
AC-FS(config)#aaa new-model AC-
FS(config)#int virtual-ppp 1
AC-FS(config-if-Virtual-ppp 1)#ppp authorization default
AC-FS(config-if-Virtual-ppp 1)#
```

【Verification】 Run the show running-config command to display the authorization list of AAA authentication of PPP configured on the current interface.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

8.5 ppp chap

Configure the username and password for PPP chap authentication.

ppp chap hostname name

ppp chap password password

Delete the configured PPP username and password.

no ppp chap hostname

【Parameter Description】

Parameter	Description
name	User name for CHAP authentication.
password	Password for CHAP authentication.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 PPP negotiation is required for both VPDN and PPPOE dialing. The second phase of PPP negotiation is about user name and password authentication. This command is used to configure the user name and password for CHAP authentication.

【Configuration Example】 The following example configures the user name and password for CHAP authentication on interface Virtual-PPP 1.

```
AC-FS(config-if-Virtual-ppp 1)#ppp chap hostname 111
AC-FS(config-if-Virtual-ppp 1)#ppp chap password 111
AC-FS(config-if-Virtual-ppp 1)#no ppp chap hostname
AC-FS(config-if-Virtual-ppp 1)#
```

【Verification】 Run the show running-config command to display the user name and password configured on the current interface for CHAP authentication.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

8.6 8.6ppp pap sent-username username password password

Configure the user name and password for PPP PAP authentication.

ppp pap sent-username username password password

Delete the username and password of the configured PPP PAP.

no ppp pap sent-username

【Parameter Description】

Parameter	Description
username	pap authenticated username.
password	password for pap authentication.

【Command Mode】 In interface configuration mode

【Default Level】 14

【Usage Guide】 VPDN and PPPOE dialing need to use PPP negotiation. The second stage of negotiation is the authentication of username and password. This command is mainly used to configure the username and password of PAP authentication.

【Configuration Example]】 1: Configure the user name and password for PAP authentication on the Virtual-PPP 1 port.

```
AC-FS(config-if-Virtual-ppp 1)#ppp pap sent-username 111 password 111
AC-FS(config-if-Virtual-ppp 1)#no ppp pap sent-username
AC-FS(config-if-Virtual-ppp 1)#
```

【Verification】 1: Use the show running-config command to view the user name and password for PAP authentication configured on the interface.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】-

8.7 ppp ipcp dns

Use this command to configure the DNS option involved in the IPCP phase of PPP negotiation.

ppp ipcp dns {A.B.C.D[A.B.C.D] [accept] | accept | request | reject }

Use this command to delete the configured DNS option.

no ppp ipcp dns {A.B.C.D[A.B.C.D] [accept] | accept | request | reject }

【Parameter Description】

Parameter	Description
accept	Receives all non-0 DNS addresses.
request	Requests the DNS address from the peer server.
reject	Refuses to negotiate the DNS option with the peer end.
A.B.C.D	DNS address.

【Command Mode】 Interface configuration mode

【Default Configuration】 The DNS option is not configured by default.

【Default Level】 14

【Usage Guide】 This command is used to configure the DNS option involved in the IPCP negotiation phase.

【Configuration Example】 The following example configures the DNS option involved in the IPCP negotiation phase.

```
AC-FS(config-if-Virtual-ppp 1)#ppp ipcp dns accept AC-
FS(config-if-Virtual-ppp 1)#ppp ipcp dns reject AC-FS(config-
if-Virtual-ppp 1)#ppp ipcp dns request AC-FS(config-if-
Virtual-ppp 1)#ppp ipcp dns 1.1.1.1 2.2.2.2 AC-FS(config-if-
Virtual-ppp 1)#no ppp ipcp dns
AC-FS(config-if-Virtual-ppp 1)#
```

【Verification】 Run the show running-config command to display whether the DNS option has been configured on the current

interface.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

8.8 ppp lcp mru negotiate

Use this command to configure the Maximum Receive Unit (MRU) option for PPP auto-negotiation.

ppp lcp mru negotiate

Use the no form of this command to remove the MRU configuration.

no ppp lcp mru

【Parameter Description】 -

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】The MRU option, as a common option involved in the PPP negotiation process, will be carried in packets from both ends during negotiation so as to determine the maximum size of packets to be transmitted on the entire link.

【Configuration Example】 The following example configures the MRU option for auto-negotiation on interface Virtual-ppp 1.

```
AC-FS(config-if-Virtual-ppp 1)#ppp lcp mru negotiate
AC-FS(config-if-Virtual-ppp 1)#
```

【Verification】 Run the show running-config command to display whether the MRU option has been configured on the current interface.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

8.9 ppp max-bad-auth

Use this command to specify the number of PPP authentication retries.

ppp max-bad-authnumber

Use the no form of this command to restore the default setting.

no ppp max-bad-auth

【Parameter Description】

Parameter	Description
number	Number of PPP authentication retries, in the range from 1 to 255.

【Default Configuration】 The default is 1.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】The number of PPP authentication retries includes the first authentication; that is, if the number of PPP authentication retries is set to 3, twice authentication is still allowed following the failure of the first authentication. When the last authentication fails, the line is interrupted (or reset).

【Configuration Example】 1.The following example sets the number of PPP authentication retries on interface virtual-ppp1 to 3:

```
AC-FS(config-if-Virtual-ppp 1)# ppp max-bad-auth 3
```

2. The following example restores the number of PPP authentication retries to the default setting.

```
AC-FS(config-if-Virtual-ppp 1)# no ppp max-bad-auth
```

【Verification】 Run the show running-config interface virtual-ppp 1command to display the configuration on the current interface.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

8.10 ppp negotiation-timeout

Use this command to specify the maximum PPP negotiation timeout period.

ppp negotiation-timeout seconds

Use the no form of this command to restore the default setting.

no ppp negotiation-timeout

【Parameter Description】

Parameter	Description
seconds	Maximum PPP negotiation timeout period, in the range from 10 to 65535 in the unit of seconds

【Default Configuration】 The default is 20 seconds.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 If the maximum negotiation timeout period expires but PPP negotiation is not finished, the PPP negotiation is considered as having failed. The maximum PPP negotiation timeout period is 20s by default.

【Configuration Example】 The following example sets the maximum PPP negotiation timeout period on interface virtual-ppp1 to 200 seconds:

```
AC-FS (config)# interface virtual-ppp 1
AC-FS(config-if-Virtual-ppp 1)# ppp negotiation-timeout 200
```

2. The following example restores the maximum PPP negotiation timeout period to the default settings.

```
AC-FS(config-if-Virtual-ppp 1)# no ppp negotiation-timeout
```

【Verification】 Run the show running-config interface virtual-ppp 1command to check the configuration on the current interface.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

9 PPPOE-CLIENT

9.1 clear dialer

Use this command to clear statistics about the DDR dialer interface.

clear dialer

【Parameter Description】 -

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 This command is used to clear the statistics information of the dial-up interface.

【Configuration Example】 1: Clear the statistics of the dial-up interface.

```
FS# clear dialer
```

【Prompt Information】-

【Platform Description】-

9.2 clear oppoe tunnel

Use this command to clear all PPPoE tunnels.

clear pppoe tunnel

【Parameter Description】 -

【Command Mode】 Privileged mode

【Usage Guide】 This command is used to clear all PPPoE tunnels.

【Configuration Example】 The following example clears all PPPoE tunnels.

```
FS# clear pppoe tunnel
```

【Prompt Information】-

【Platform Description】-

9.3 dialer enable-timeout

Configure the line invalid time.

dialer enable-timeout seconds

Restore the default value of line invalid time.

no dialer enable-timeout

【Parameter Description】

Parameter	Description
seconds	Line inactive time (seconds)..

【Default Configuration】15 seconds.

【Command Mode】 Interface mode

【Default Level】 14

【Usage Guide】 The line invalid time is the waiting time of the interface after the line is cut off or the dialing fails before the interface can dial, that is, the waiting time of the interface before dialing again.

【Configuration Example】 1. The following example configures the timeout period for the ASDL line to 20 seconds.

```
FS(config)# interface dialer 1
FS(config-if-dialer 1)# dialer enable-timeout 20
```

2. The following example restores the timeout period for the ASDL line to the default setting.

```
FS(config)# interface dialer 1
FS(config-if-dialer 1)# no dialer enable-timeout
```

【Verification】1: Use the show running-config interface dialer 1 command to check whether the configuration exists.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

9.4 dialer-group

The rules associated with interface stimulus dialing.

dialer-group group-number

Delete the dial stimulus rule associated with the dial port.

no dialer-group

【Parameter Description】

Parameter	Description
group-number	The number of the stimulus dial plan.

【Default Configuration】 There is no associated dial rule.

【Command Mode】 Interface mode

【Default Level】 14

【Usage Guide】If you try to dial an interface, you must first determine what packets can stimulate dialing. The stimulating dialing rules are specified by the global configuration command dialer-list, and then associate one of the dialing rules on the interface.

【Configuration Example】1: The dialer 1 port is associated with the interface to stimulate dialing rule 1.

```
FS(config)# interface dialer 1
FS(config-if-dialer 1)# dialer-group 1
```

2: Delete the stimulus dialing rules associated with the dialer 1 port.

```
FS(config)# interface dialer 1
FS(config-if-dialer 1)# no dialer-group
```

【Verification】1: Use the show running-config interface dialer 1 command to check whether the configuration exists.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

9.5 dialer hold-queue

Configure the hold queue for the interface.

dialer hold-queue packets [timeout seconds]

Close the hold queue.

no dialer hold-queue [packets [timeout seconds]]

【Parameter Description】

Parameter	Description
packets	Sets the number of packets the queue can hold, in the range from 0 to 100.
timeout seconds	Sets the timeout period of the hold queue, in the unit of seconds. The default is 45 seconds.

【Default Configuration】 Close the hold queue.

【Command Mode】 Interface mode

【Default Level】 14

【Usage Guide】 It takes a period of negotiation time for the device to use the MODEM dial-up to connect, during which the packets will be discarded. However, if the hold queue is configured, the packets equipped with the stimulus dialing rules can be stored on the device

and sent immediately after the connection is established.

【Configuration Example】 1. The following example sets the hold queuepacketsto 50.

```
FS(config)# interface dialer 1
FS(config-if-dialer 1)# dialer hold-queue 50
```

2. The following example restores the default setting.

```
FS(config)# interface dialer 1
FS(config-if-dialer 1)# no dialer hold-queue
```

【Verification】 1: Use the show running-config interface dialer 1 command to check whether the configuration exists.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

9.6 dialer idle-timeout

Configure the line idle time.

dialer idle-timeout seconds

Restore the default value of line idle time.

no dialer idle-timeout

【Parameter Description】

Parameter	Description
seconds	Line idle time (seconds).

【Default Configuration】 120 seconds.

【Command Mode】 Interface mode

【Default Level】 14

【**Usage Guide**】Line idle time specifies how long the dial-up line will cut off the line when there is no data communication. During this period, when a message to the destination address is received, the line idle time will be reset.

【**Configuration Example**】 1. The following example sets the idle period to 60 seconds.

```
FS(config)# interface dialer 1
FS(config-if-dialer 1)# dialer idle-timeout 60
```

2. The following example restores the default setting.

```
FS(config)# interface dialer 1
FS(config-if-dialer 1)# no dialer idle-timeout
```

【**Verification**】1: Use the show running-config interface dialer 1 command to check whether the configuration exists.

【**Prompt Information**】-

【**Common Mistake**】-

【**Platform Description**】 Gateway EG/NBR/NPE series products.

9.7 dialer-list

Define the rules for stimulus dialing.

dialer-list dialer-group protocol protocol-name ip { permit | deny | list access-list-number }

Deletes the specified stimulus dial plan.

no dialer-list dialer-group [protocol protocol-name ip { permit | deny | list access-list-number }]

【**Parameter Description**】

Parameter	Description
dialer-group	The number of the stimulus dial plan.
protocol protocol-name	Protocol name.
ip	Allowed is the IP protocol
permit	The entire IP protocol is allowed.
deny	Deny the entire IP protocol.
list	Use access lists instead of entire protocols to define stimulus dialing rules.

access-list-number	The number of the access list.

【Default Configuration】 No stimulus dialing rules are defined.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 This command defines one or more stimulus dial rules in global configuration mode, and then uses dialer-group to apply dial rules to specific interface dialing. It is one of the commands that must be configured for dialing out.

【Configuration Example】1: Configure dial stimulus rule 1 to allow IP protocol packets.

```
FS(config)# dialer-list 1 protocol ip permit
```

2: Delete dial stimulus rule 1.

```
FS (config)# no dialer-list 1
```

【Verification】1: Use the show running-config | include dialer-list 1 command to check whether the configuration exists.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

9.8 dialer pool

Configure the dial-up pool associated with the logical port.

dialer pool number

Cancel the dial pool associated with the logical port.

no dialer pool number

【Parameter Description】

Parameter	Description
number	Sets the ID of a dialer pool, in the range from 1 to 255.

【Default Configuration】 No dialing pool is associated.

【Command Mode】 Interface mode

【Default Level】 14

【Usage Guide】 In advanced dialing, the logical interface must be associated with a specific physical port to perform actual dialing. In order to establish the association between the logical interface and the physical interface, the dial pool is used. First, add a specific physical interface to one or more dial-up pools, and then associate one of the dial-up pools on the logical interface, thereby realizing the association between the logical interface and the physical interface. A physical interface can belong to multiple dial-up pools, but a logical interface can only be associated with one dial-up pool. When a logical interface performs specific dialing, it randomly selects an idle interface in the dial-up pool for dialing.

【Configuration Example】 1. The following example associates dialer pool 1 with dialer interface1.

```
FS(config)# interface dialer 1
FS(config-if-dialer 1)# dialer pool 1
```

2 The following example restores the default setting.

```
FS(config)# interface dialer 1
FS(config-if-dialer 1)# no dialer pool
```

【Verification】1: Use the show running-config interface dialer 1 command to check whether the configuration exists.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

9.9 ip address

Configure the interface IP policy.

ip address { negotiate | ip-addr subnet-mask }

Delete the interface IP policy.

no ip address

【Parameter Description】

Parameter	Description
negotiate	Enables an interface to acquire IP address through PPP negotiation.
ip-addr	The IP address of a specified interface.
subnet-mask	The mask of a specified interface.

【Default Configuration】 There is no default value.

【Command Mode】 Interface mode

【Default Level】 14

【Usage Guide】 This command is mainly used to specify how to obtain the logical interface IP.

If you choose to obtain the address through PPP negotiation, the IP of the logical interface is assigned by the server.

If you manually specify the IP of the logical interface, you need to obtain the consent of the server during the negotiation process before the specified IP can take effect.

【Configuration Example】 1. The following example sets the IP policy to PPP negotiation.

```
FS(config)# interface dialer 1
FS(config-if-dialer 1)# ip address negotiate
```

2. The following example removes the IP policy configuration.

```
FS(config)# interface dialer 1
FS(config-if-dialer 1)# no ip address
```

【Verification】 1: Use the show running-config interface dialer 1 command to check whether the configuration exists.

2: Use the show ip interface brief | in dialer 1 command to check whether the configuration has been negotiated to IP and the protocol has been UP.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】-

9.10 ppp max-bad-auth

Specifies the number of retries for PPP authentication.

ppp max-bad-auth number

Restore the PPP authentication retries to the default value.

no ppp max-bad-auth

【Parameter Description】

Parameter	Description
number	Sets PPP authentication retry count, in the range from 1 to 255.

【Default Configuration】 Do not retry.

【Command Mode】 Interface mode

【Default Level】 14

【Usage Guide】 The number of retries includes the first authentication, that is, if the number of retries is set to 3, after the first authentication fails, you can re-authenticate 2 times. After the last authentication failure, the line is hung up (reset).

【Configuration Example】 1. The following example sets PPP authentication retry count to 3.

```
FS(config)# interface dialer 1
FS(config-if-dialer 1)# ppp max-bad-auth 3
```

2. The following example restores the default setting.

```
FS(config)# interface dialer 1
FS(config-if-dialer 1)# no ppp max-bad-auth
```

【Verification】1: Use the show running-config interface dialer 1 command to check whether the configuration exists.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

9.11 pppoe enable

Enable the PPPoE function of the interface.

pppoe enable

Disable the PPPoE client function of the interface.

no pppoe enable

【Parameter Description】 -

【Command Mode】 Interface configuration mode

【Default Configuration】 This function is disabled by default

【Usage Guide】Use this command on physical or aggregate WAN interfaces.

【Configuration Example】 1. The following example enables the PPPoE client function on Gigabit Ethernet 0/5.

```
FS(config)# interface GigabitEthernet 0/5
FS(config-if- GigabitEthernet 0/5)# pppoe enable
```

2. The following example restores the default setting.

```
FS(config)# interface GigabitEthernet 0/5
FS(config-if- GigabitEthernet 0/5)# no pppoe enable
```

【Verification】1: Use the show running-config interface GigabitEthernet 0/5 command to check whether the configuration exists.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

9.12 pppoe-client dial-pool-number

Add the Ethernet port to the dial-up pool and configure the dial-up type.

pppoe-client dial-pool-number number no-ddr

Take the Ethernet port out of the dial-up pool and delete its dial-up policy.

no pppoe-client dial-pool-number number

【Parameter Description】

Parameter	Description
number	Dial pool number.
no-ddr	Use automatic dialing.

【Default Configuration】 Close.

【Command Mode】 Interface mode

【Default Level】 14

【Usage Guide】 Use this command to bind the Ethernet port to a specified dial-up pool, and the logical interface uses the specified dial-up pool, so as to establish an association between the Ethernet port and the logical interface to realize dialing. Before configuring this command, the interface must be configured with pppoe enable.

【Configuration Example]】1: Configure GigabitEthernet 0/5 to join dial pool 1.

```
FS(config)# interface GigabitEthernet 0/5
FS(config-if- GigabitEthernet 0/5)# pppoe-client dial-pool-number 1 no-ddr
```

2: Delete the IP policy of the dialer 1 port.

```
FS(config)# interface GigabitEthernet 0/5
FS(config-if- GigabitEthernet 0/5)# no pppoe-client dial-pool-number 1
```

【Verification】1: Use the show running-config interface GigabitEthernet 0/5 command to check whether the configuration exists.

【Prompt Information】 1: The interface needs to enable the PPPoE function first.

```
PPPoE: must enable PPPoE firstly.
```

【Common Mistake】-

9.13 pppoe multi-dial enable

Use this command to enable the PPPoE client multi-dial function of the device. That is, multiple channels of PPPoE dialup can be configured on a physical port. If the function is disabled, only one channel of PPPoE dialup can be used on each physical port.

pppoe multi-dial enable

Use the no form of this command to disable the PPPoE client multi-dial function of the device.

no pppoe multi-dial enable

【Parameter Description】 -

【Command Mode】 Global configuration mode

【Default Configuration】 The PPPoE client multi-dial function is disabled on the device by default.

【Default Level】 14

【Usage Guide】 This command is used to enable the PPPoE client multi-dial function and the function is disabled by defaults.

【Configuration Example】 1. The following example enables the PPPoE client multi-dial function of the device in global configuration mode.

```
FS(config)# pppoe multi-dial enable
```

2. The following example disables the PPPoE client multi-dial function of the device.

```
FS(config)# no pppoe multi-dial enable
```

【Verification】 1: Use the show running-config command to check whether the configuration exists.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

9.14 pppoe session mac-address

Use this command to configure the MAC address of a PPPoE session.

pppoe session mac-addressH.H.H

Use the no form of this command to restore the default setting.

no pppoe session mac-address

【Parameter Description】

Parameter	Description
H.H.H	Configures the MAC address of a PPPoE session.

【Command Mode】 Interface configuration mode

【Default Configuration】 This function is disabled by default..

【Default Level】 14

【Usage Guide】 Use this command to specify the mac address of the pppoe dial-up session. The configuration can be configured under the interface, but the configuration can only take effect under the sub-interface. Before configuring the mac address of the session on the sub-interface, the pppoe function must be enabled on the interface.

【Configuration Example】 1: Configure the mac address of the pppoe session of GigabitEthernet 0/5.1 as 00d0.f822.33f3.

```
AC-FS (config)# interface GigabitEthernet 0/5.1 AC-
FS(config-subif-GigabitEthernet 0/5.1)#pppoe enable
AC-FS(config-subif-GigabitEthernet 0/5.1)#encapsulation dot1Q 1
AC-FS(config-subif-GigabitEthernet 0/5.1)#pppoe sessiom mac-address 00d0.f822.33f3
```

2: Delete the IP policy of the dialer 1 port.

```
AC-FS (config)# interface GigabitEthernet 0/5.1
AC-FS(config-subif-GigabitEthernet 0/5.1)#no pppoe sessiom mac-address
```

【Verification】 1: Use the show running-config interface GigabitEthernet 0/5.1 command to check whether the configuration exists.

【Prompt Information】 1: The interface needs to enable the PPPoE function first.

PPPoE: must enable PPPoE firstly.

【Common Mistake】-

【Platform Description】-

9.15 show pppoe

View information about PPPoE sessions.

show pppoe { ref | session | tunnel }

【Parameter Description】

Parameter	Description
ref	Display fast forward information for all PPPoE sessions.
session	Display all PPPoE session information.
tunnel	Display all PPPoE tunnel information.

【Command Mode】 Privileged EXEC mode/Global configuration mode/Interface configuration mode

【Default Configuration】 This function is disabled by default.

【Default Level】 14

【Usage Guide】 N/A

【Configuration Example】 1: Display fast forward information of all PPPoE sessions.

```
FS# show pppoe ref

 GigabitEthernet 0/6 Virtual-pppoe 2 dialer 1
  Protocol UP dialer-group 1 last_time 164235070 ms
  Ether Header: 00 60 4F 67 02 50 00 D0 F8 22 33 43 88 64
  PPPoE Header: 11 00 00 7F 00 50
  PPP Header  : 00 21
  DstMac 0060.4f67.0250, SrcMAC 00d0.f822.3343, SessionID 127
  Input Err : 0 MAC, 0 PPPoE Header
  Input Info: 0 Normal, 0 Drop, 345 Reserve, 0 Lost
  Output Err : 0 SessionState, 0 no ref, 0 length
  Output Info: 0 Normal, 0 Drop, 0 Reserve, 0 Lost

 There is 1 pppoe session in System
```

Field Description: Because the information itself has been described very clearly, it will not be repeated here.

2: Display all PPPoE session information

```
FS# show pppoe session
state is SESSION ,my mac is 00.D0.F8.22.33.43 , peer mac is 00.60.4F.67.02.50
   Timer is running: 59750
```

Field Description: Because the information itself has been described very clearly, it will not be repeated here.

3: Display all PPPoE tunnel information.

```
FS# show pppoe tunnel
state is SESSION ,my mac is 00.D0.F8.22.33.43 , peer mac is 00.60.4F.67.02.50
   Timer is running: 59003
```

Field Description: Because the information itself has been described very clearly, it will not be repeated here.

【Prompt Information】-

【Platform Description】-

10 PPPoE-SERVER

10.1 ac-cookie enable

Use this command to enable the AC cookie function in bba-group configuration mode.

ac-cookie enable

Use the no form of this command to disable the AC cookie function.

no ac-cookie enable

Use the no form of this command to restore the default configuration.

no ac-cookie enable

【Parameter Description】 -

【Default Configuration】 Disable ac-cookie.

【Command Mode】 bba-group

【Default Level】 14

【Usage Guide】 This command is used to enable the ac-cookie function in the configured bba-group pppoe group.

【Configuration Example】Example 1: The following example will enable the ac-cookie functionality:

```
AC-FS(config)# bba-group pppoe pppoe_server_group
AC-FS(config-bba-group)# ac-cookie enable
```

【Verification】 1: Use the show run command to check whether ac-cookie is enabled or disabled.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

10.2 baa-group pppoe

To set the bba-group pppoe dial-up group, execute the bba-group pppoe command in the global configuration mode. The no form of this command deletes the specified bba group.

bba-group pppoe bba-group-name

delete bba-group.

no bba-group pppoe bba-group-name

Restore Default Configuration.

default bba-group pppoe bba-group-name

【Parameter Description】

Parameter	Description
bba-group-name	Indicates the name of a bba-group.

【Default Configuration】 The bba-group is not configured by default.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 This command is used to configure bba-group pppoe group, which is used for dial-up of pppoe-server. bba-group-name can only be configured with a maximum of 32 characters.

【Configuration Example】 Example 1: The following example will configure a bba-group:

```
AC-FS(config)# bba-group pppoe pppoe_server_group
```

【Verification】 1: Use the show run command to view the bba-group configuration.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

10.3 pppoe-server enable

To use the pppoe server function, perform the pppoe-server enable command that turns off the pppoe server function in its no form.

pppoe-server enable

Turn off the pppoe server function.

no pppoe-server enable

Restore the Default Configuration.

default pppoe-server enable

【Parameter Description】

Parameter	Description
pppoe-server enable	Global enables PPPoE Server functionality.

【Default Configuration】 By default, the function of pppoe server is not enabled.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Global configuration command, to use the function of pppoe server, please execute this command in global mode. After the shutdown, the packets of the pppoe server are no longer processed.

【Configuration Example】 #Configure a bba-group.

```
AC-FS(config)#pppoe-server enable
```

【Verification】 1: Use the show run command to check whether the PPPoE Server function is enabled.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

10.4 pppoe-server enable group

To use the pppoe server function, perform the pppoe-server enable command that turns off the pppoe server function in its no form.

pppoe-server enable

Turn off the pppoe server function.

no pppoe-server enable

Restore the Default Configuration.

default pppoe-server enable

【Parameter Description】

Parameter	Description
group-name	Indicates the bba-group dialup group associated with this interface.

【Command Mode】 Interface configuration mode

【Default Configuration】 The PPPoE server function of an interface is disabled by default.

【Default Level】 14

【Usage Guide】 Use this command to enable the PPPoE server function in interface configuration mode for a L3 physical interface, L3 sub interface, or SVI. The name of a bba-group contains no more than 32 characters. The PPPoE server function can be enabled on the SVI only for wireless products.

【Configuration Example】 Example 1: The following example demonstrates enabling the pppoe server function on vlan 3.

```
AC-FS(config)# interface vlan 3
AC-FS(config-if-VLAN 3)# pppoe-server enable group pppoe_server_group
```

【Verification】 1: Use the show run or show interface command to check whether the pppoe-server is enabled on the interface.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

10.5 sessions local-mac limit

To configure the maximum number of sessions that the same mac address of the local end can accept incoming calls on the interface associated with the current bba-group group, specify the

Configure the sessions local-mac limit command under the bba-group group. The no form of this command is restored to the default value.

sessions local-mac limit limit-count

Restore default values.

no sessions local-mac limit

Restore Default Configuration.

default sessions local-mac limit

【Parameter Description】

Parameter	Description
limit-count	Indicates the maximum number of sessions that can be received at a local MAC address. The value range is from 0 to 1,000.

【Command Mode】 bba-group

【Default Configuration】 The maximum number of sessions that can be received at a local MAC address is 1,000 by default..

【Default Level】 14

【Usage Guide】 Use this command to configure, in bba-group configuration mode, the maximum number of sessions that can be received at a local MAC address. Changing this parameter does not affect established sessions and the changed parameter takes effect only on the next established session.

If this parameter is set to 0, the current interface does not allow PPPoE dialup.

【Configuration Example】 #Set the maximum number of sessions that can be received at the local MAC address associated with the pppoe_server_group to 50.

```
AC-FS(config)# bba-group pppoe pppoe_server_group
AC-FS(config-bba-group)# sessions local-mac limit 50
```

【Verification】1: Use the show run command to view the number of sessions per-mac under bba-group.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

10.6 sessions max limit

To configure the maximum number of sessions allowed by the current system, configure the sessions max limit command in bba-group mode, and the no form of this command returns to the default value.

sessions max limit limit-count

Restore default values.

no sessions max limit

Restore Default Configuration.

no sessions max limit

【Parameter Description】

Parameter	Description
limit-count	Indicates the maximum number of sessions that can be received by the current system. The value range is from 0 to 1,000.

【Command Mode】 bba-group

【Default Configuration】 The maximum number of sessions that can be received by the current system is 1,000 by default.

【Default Level】 14

【Usage Guide】Use this command to configure, in bba-group configuration mode, the maximum number of sessions that can be received by the local system.

Changing this parameter does not affect established sessions and the changed parameter takes effect only on the next established session.

If this parameter is set to 0, the current interface does not allow PPPoE dialup. Configure this parameter in bba-group configuration mode to validate the value to all bba-groups. The value will be displayed under all bba-groups. The latest configured value prevails.

【Configuration Example】 #Set the maximum number of sessions that can be received by the current system to 500.

```
AC-FS(config)# bba-group pppoe pppoe_server_group
AC-FS(config-bba-group)# sessions max limit 500
```

【Verification】 1: Use the show run command to view the configuration of the sessions max limit of bba-group.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

10.7 sessions per-mac limit

To configure the maximum number of sessions that can be dialed in by the same mac address of the peer end on the interface associated with the current bba-group group, specify the

Configure the sessions per-mac limit command under the bba-group group. The no form of this command is restored to the default value.

sessions per-mac limit limit-count

Restore default values.

no sessions per-mac limit

Restore Default Configuration.

no sessions per-mac limit

【Parameter Description】

Parameter	Description
limit-count	Indicates the maximum number of sessions that can be initiated from a peer MAC address. The value range is from 0 to 500.

【Command Mode】 bba-group

【Default Configuration】 The maximum number of sessions that can be initiated from a peer MAC address is 100 by default.

【Default Level】 14.

【Usage Guide】Use this command to configure, in bba-group configuration mode, the maximum number of sessions that can be initiated from a peer MAC address. Changing this parameter does not affect established sessions and the changed parameter takes effect only on the next established session. If this parameter is set to 0, the current interface does not allow PPPoE dialup.

【Configuration Example】 #Set the maximum number of sessions that can be initiated from the peer MAC address associated with the pppoe_server_group to 50.

```
AC-FS(config)# bba-group pppoe pppoe_server_group
AC-FS(config-if)# sessions per-mac limit 50
```

【Verification】1: Use the show run command to view the configuration of sessions per-mac limit

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

10.8 virtual-template

To specify the virtual-template interface associated with the current bba-group pppoe group, execute virtual-template under the bba-group pppoe group command, the no form of the command removes the association.

virtual-template interface-number

Remove virtual-template.

no virtual-template interface-number

Restore Default Configuration.

default virtual-template interface-number

【Parameter Description】

Parameter	Description
interface-number	Indicates the serial number of an interface.

【Default Configuration】 By default, the virtual-template interface is not associated.

【Command Mode】 bba-group

【Default Level】 14

【Usage Guide】To associate a virtual-template interface under the specified bba-group group, execute this command in bba-group pppoe mode.

【Configuration Example】 #Specify virtual template interface 5 to associate with a bba-group PPPoE group.

```
AC-FS(config)# bba-group pppoe pppoe_server_group
AC-FS(config-bba-group)# virtual-template 5
```

【Verification】1: Use the show run command to view the configuration under bba-group.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

10.9 show pppoe-server

To view status information for the PPPOE SERVER, execute the privileged user mode command show pppoe-server command.

show pppoe-server { ref | session | tunnel } [session-id sid]

【Parameter Description】

Parameter	Description
ref	Displays all session information on the data plane.

session	Displays PPPoE session information.
tunnel	Displays PPPoE tunnel information.
session-id	Displays information about the specified session ID.
sid	Indicates the session ID.

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】 14

【Usage Guide】 The session and tunnel status information of this command are the same.

【Configuration Example】 #Run the show pppoe-server ref command to display session information.

```
AC-FS#show pppoe-server  ref
PPPOE Server ref current sessions count : 4
```

```
Sid: 2,In Intf:virtual-access 1,Out Intf:CAPWAP-Tunnel 1
LocalMAC:00-1A-A9-7C-B2-DD,RemoteMAC: C8-3A-35-C3-01-AC
             Input Info: 13 Normal, 0 Drop, 16 Reserve, 0 Lost
             Output Info: 0 Normal, 0 Drop, 0 Reserve, 0 Lost

Sid: 3,In Intf:virtual-access 2,Out Intf:CAPWAP-Tunnel 1
LocalMAC:00-1A-A9-7C-B2-DD,RemoteMAC: D8-5D-4C-7F-10-0A
             Input Info: 2 Normal, 0 Drop, 13 Reserve, 0 Lost
             Output Info: 0 Normal, 0 Drop, 0 Reserve, 0 Lost

Sid: 4,In Intf:virtual-access 0,Out Intf:CAPWAP-Tunnel 1
LocalMAC:00-1A-A9-7C-B2-DD,RemoteMAC: C8-3A-35-C0-B4-FC
             Input Info: 7 Normal, 0 Drop, 7 Reserve, 0 Lost
             Output Info: 0 Normal, 0 Drop, 0 Reserve, 0 Lost
```

【Field Description】

Field	Description
PPPOE Server ref current sessions count	The total number of sessions established by the data plane.
Sid	session id.
In Intf	The virtual interface corresponding to the current session to receive

	packets.
Out Intf	The physical interface on which the current session transmits packets.
LocalMAC	The mac address of the local interface.
RemoteMAC	Session remote interface mac address.
Input Info	Inbound packet statistics.
Normal	Number of packets received normally.
Drop	Number of discarded received abnormal packets.
Reserve	Number of received packets sent to the control plane.
Lost	The number of lost packets received.
Output Info	Outbound packet statistics.
Normal	Number of messages sent normally.
Drop	Number of discarded abnormal packets sent.
Reserve	Number of packets sent to the control plane.
Lost	The number of lost sent packets.

Example 2: The following example is an execution result of show pppoe-server session.

```
AC-FS#show pppoe-server session
```

```
#The following is the information related to pppoe server


Sid    State               intf                external-vid     inner-vid     Peer
LocalMAC           RemoteMAC          online time
20     STATE_SESSION       virtual-access 5091   1             0.....7.7.7.2
00:D0:F8:22:12:81  08:FB:0A:B0:48:AF  0 day(s) 15:16:31


PPPOE Server current sessions count : 1
```

Field Description

Field	Description
PPPOE Server current sessions count t	The total number of sessions established by the control plane.
Sid	Session id

State	STATE_SENT_IDLE idle STATE_SENT_PADI Send PADI STATE_RECEIVED_PADI Receive PADI STATE_SEND_PADO Send PADO STATE_RECEIVED_PADO Receive PADO STATE_SENT_PADR Send PADR STATE_RECEIVED_PADR Receive PADR STATE_SEND_PADS Send PADS STATE_SESSION Enter SESSION stage STATE_TERMINATED SESSION terminated
intf	The interface corresponding to the current session.
External vid	encapsulated vlan id.
Inner vid	The inner vlan id in the QINQ scenario currently does not support QINQ termination, so it is always 0.
PeerIP	IP address assigned to pppoe client.
LocalMAC	The mac address of the local interface.
RemoteMAC	Session remote interface mac address.
online time	The online duration of the current session.

【Prompt Information】-

【Platform Description】-

Chapter 7 IP address and Application

This volume introduces the relevant contents of the IP address and application command manual, including the following chapters:

1. IP address / service
2. ARP
3. DHCP
4. DNS
5. FTP-Server
6. FTP Client
7. TUNNEL
8. Network connectivity test tool
9. TCP
10. Software IPv4 fast turn
11. TFTP-Server
12. NAT
13. DDNS

1 IP address/server

1.1 ap-interface bvi num ip address

Configure the ip address for the BVI port of the specified AP.

ap-interface bvi num ip address {ip-address network-mask | dynamic}

Remove the SVI port ip address for the specified AP.

no ap-interface bvi num ip address

【Parameter Description】

Parameter	Description
num	The ap-end bvi port port number.
ip-address	The 32 bit-bit IP addresses, the 8-bit group, are represented in a decimal fashion, and the groups are separated by points.
network-mask	32 bit network masks, "1" indicates the mask bit and "0" indicates the host bit.Each 8 groups, represented in decimal fashion, between groups separated by points.
dynamic	Configure the ap-end bvi port ip address and the mask by dynamically acquiring the ip and the mask.

【Default Configuration】 Default is not configured

【Command Mode】 Issue ap based on ap-config / ap-group modes

【Default Level】 2

【Usage Guide】 The command is configured in both ap-config / ap-group modes, where ap-config is again divided into two modes: ap-config all and ap-config apname.The priorities configured on the AC are ranked from high to low as ap-config apname, ap-group, ap-config all, and each mode allows only one ip address on one bvi port. The AC selects the allocation with the highest priority to the pair according to the priority of the AP mode

When the AP adopts the thin AP local forwarding networking mode, if the ap-interface bvi num ip address ip-address network-mask configuration is used, the APs need to be divided into different VLANs, otherwise there will be address conflicts, use the ap-interface bvi num ip address dynamic does not have this restriction.

【Configuration Example】 1: The ip address of the bvi 2 port configured with ap in ap-config ap120 mode is 192.168.2.1 255.255.255.0.

```
AC-FS(config)#ap-config ap120
You are going to config AP(ap120), which is online now.
AC-FS(config-ap)#ap-interface bvi 2 ip address 192.168.2.1 255.255.255.0
```

2: The ip address of the bvi 3 port configured with ap in ap-group mode is 192.168.3.1 255.255.255.0

```
AC-FS(config)#ap-group default
AC-FS(config-group)#ap-interface bvi 3 ip address 192.168.3.1 255.255.255.0
```

.

3: The ip address of the bvi 4 port configured with ap in ap-config all mode is 192.168.4.1 255.255.255.0.

```
AC-FS(config)#ap-config all
AC-FS(config-ap)#ap-interface bvi 4 ip address 192.168.4.1 255.255.255.0
```

4: The ip address of the bvi 4 port of the ap in ap-config all mode is dynamically obtained according to the mac address of the ap.

```
AC-FS(config)#ap-config all
AC-FS(config-ap)#ap-interface bvi 4 ip address dynamic
```

【Verification】 AC show run or show ap-config run shows the corresponding configuration, and AP terminal show ip interface brief shows the IP address of the effective BVI interface.

【Prompt Information】 1. If the configured ip address is illegal, the following prompt appears:

Invalid IP address.

2. If the address mask is configured, the following prompt appears:

Invalid IP mask.

3. An ap configuration mode allows only ip address for one bvi port, prompted when ip address on different bvi ports:

Please remove ip address on bvi 2 first.

【Common Mistake】 -

【Platform Description】 -

1.2 ip-address

Configure the IP address of the interface.

ip address ip-address network-mask [secondary]

Deletes the IP address of the specified interface.

no ip address [ip-address network-mask [secondary]

【Parameter Description】

Parameter	Description
ip-address	A 32-bit IP address, in groups of 8, expressed in decimal, and the groups are separated by dots.
network-mask	32 bit netmask, "1" for mask bit, "0" for host bit. Groups of 8 bits, expressed in decimal, separated by dots.
secondary	Indicates the configured secondary IP address. The default is to configure the primary ip address.

【Default Configuration】 The interface is not configured with an IP address.

【Command Mode】 Interface mode

【Default Level】 2

【Usage Guide】 A device can receive and send IP datagrams only when it is configured with an IP address. The interface is configured with an IP address.

The netmask is also a 32-bit value that identifies which bits of the IP address are the network portion. In the network mask, the IP address bits corresponding to the bits with a value of "1" are the network part, and the IP address bits corresponding to the bits with a value of "0" are the host address part. For example, the network mask corresponding to a class A network is "255.0.0.0". You can use a network mask to subnet a network. Subnetting is to use some bits of a host address part as a network part to reduce the host capacity and increase the number of networks. At this time, the network mask is called Subnet mask.

FSOS software can support one interface to configure multiple IP addresses, one of which is the primary IP address, and the rest are all secondary IP addresses. Theoretically, there is no limit to the number of secondary IP addresses, which can be configured at will, but only after the primary IP address is configured can the secondary IP address be configured. The secondary IP address must belong to a different network from the primary and secondary IP addresses. In network construction, the secondary IP address is often used. Usually, the secondary IP address should be considered in the following situations:

A network does not have enough host addresses. Now the general local area network needs a class C network, which can allocate 254 hosts. But when there are more than 254 LAN hosts, a class C network will not be enough to allocate, and it is necessary to allocate another class C network address. In this way, the device needs to be connected to two networks, so multiple IP addresses need to be

configured.

Many legacy networks are layer 2 bridged networks without subnetting. The use of secondary IP addresses allows the network to be easily upgraded to a routed network based on the IP layer. For each subnet, the device is configured with an IP address.

Two subnets of one network are isolated by another network. You can create a subnet of the isolated network and connect the isolated subnets by configuring the secondary IP address. A subnet cannot appear on two or more interfaces of the device

【Configuration Example】 1: The primary IP address of the interface is configured as 10.10.10.1, and the netmask is 255.255.255.0.

```
AC-FS(config)# interface gigabitEthernet 0/1
AC-FS(config-if-GigabitEthernet 0/1)# ip address 10.10.10.1 255.255.255.0
```

【Verification】 1: show ip interface to see the configuration of the interface.

【Prompt Information】 4. It is not allowed to configure a mask with all 1s or all 0s (the loopback interface can support a 32-bit mask). If it is configured, the following prompt will appear:

Invalid IP mask.

5. It is not allowed to configure the secondary ip address if the primary ip address is not configured, otherwise the following prompt will appear:

Cannot add IP address.

【Common Mistake】 1. Configure the secondary ip address if the primary ip address is not configured.

2. All slave addresses are not deleted before deleting the master address.

3. The network segments of different IP addresses on the same interface overlap.

1.3 ip address negotiate

Configure to obtain the IP address of the interface through PPP negotiation.

ip address negotiate

Delete the IP address of the interface obtained through PPP negotiation.

no ip address negotiate

【Parameter Description】 -

【Default Configuration】 The interface is not configured to obtain an IP address through PPP negotiation.

【Command Mode】 Interface mode

【Default Level】 2

【Usage Guide】 Only the point-to-point interface of the router supports obtaining an IP address through PPP negotiation. After configuring ip address negotiate on the interface, the peer end needs to configure the peer default ip address.

【Configuration Example】 The following example obtains an IP address for the interface through PPP negotiation.

```
AC-FS(config)# interface dialer 1
AC-FS(onfig-if-dialer 1)# ip address negotiate
```

【Verification】1: show ip interface to see the configuration of the interface.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.4 ip address-pool local

Enable the IP address pool function.

ip address-pool local

Disable the IP address pool function.

no ip address-pool local

【Parameter Description】 -

【Default Configuration】 The IP address pool function is enabled by default

【Command Mode】 Global configuration mode

【Default Level】 2

【Usage Guide】 By default, the IP address pool function is enabled, the user can configure the IP address pool, and the PPP user can use the IP address pool to assign the IP address of the peer. If you want to disable the IP address pool function, you can use the no ip address-pool local command, which will delete all previously configured IP address pools.

【Configuration Example】 The following example enables the IP address pool function.

```
AC-FS(config)# ip address-pool local
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.5 ip broadcast-address

Configure the broadcast address of an interface.

ip broadcast-address ip-address

Cancel the broadcast address configuration.

no ip broadcast-address

【Parameter Description】

Parameter	Description
ip-address	Broadcast address of IP network.

【Default Configuration】 The default IP broadcast address is 255.255.255.255.

【Command Mode】 Interface mode

【Default Level】 2

【Usage Guide】Currently, the destination address of IP broadcast packets is generally all "1", which is expressed as 255.255.255.255. FSOS software can generate broadcast packets of other IP addresses by definition, and can receive all "1" and self-defined broadcast packets at the same time.

【Configuration Example】 The following example sets the destination address of IP broadcast packets generated by this interface to 0.0.0.0.

```
AC-FS(config)# interface gigabitEthernet 0/1
AC-FS(config-if-GigabitEthernet 0/1)# ip broadcast-address  0.0.0.0
```

【Verification】-

【Prompt Information】 1. If the primary ip address is not configured, the broadcast configuration under the interface cannot be configured, otherwise the following prompt will appear:

```
Cannot set broadcast address. No primary address exist.
```

【Common Mistake】-

【Platform Description】-

1.6 ip icmp error-interval

Configure the sending rate of ICMP destination unreachable packets triggered by the unfragmentable bit in the IP header.

ip icmp error-interval DF milliseconds [bucket-size]

Set the sending rate of other ICMP error messages.

ip icmp error-interval milliseconds [bucket-size]

Restore the sending rate of ICMP destination unreachable packets triggered by the unfragmentable bit in the IP header to the default value.

no ip icmp error-interval DF milliseconds [bucket-size]

Restore the sending rate of other ICMP error packets to the default value.

no ip icmp error-interval milliseconds [bucket-size]

【Parameter Description】

Parameter	Description
milliseconds	The refresh period of the token bucket, the value range is 0~2147483647, the default value is 100, and the unit is milliseconds. When the value is 0, it means that the sending rate of ICMP error packets is not limited.
bucket-size	The number of tokens in the token bucket, ranging from 1 to 200. The default value is

	10.

【Default Configuration】 Send 10 in 100ms.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】To prevent denial of service attacks, the token bucket algorithm is used to limit the sending rate of ICMP error packets. If the IP packet needs to be fragmented, but the unfragmentable bit in the IP header is set, the device will send an ICMP destination unreachable packet numbered 4 to the source IP address. The main purpose of this ICMP error packet is path MTU discovery. . In order to prevent too many other ICMP error packets, the ICMP destination unreachable packet numbered 4 cannot be sent, and thus the path MTU discovery function fails, the ICMP destination unreachable packet numbered 4 and other ICMP error packets are separated. speed limit. Because the precision of the timer is 10 milliseconds, it is recommended that users configure the refresh period of the token bucket to be an integer multiple of 10 milliseconds. If the refresh cycle of the token bucket

Greater than 0, less than 10, the actual effective refresh period is 10 milliseconds, for example, if 1 is configured in 5 milliseconds, the actual effect is 2 in 10 milliseconds; if the token

The refresh period of the bucket is not an integer multiple of 10 milliseconds. The actual refresh period is automatically converted into an integer multiple of 10 milliseconds. For example, configure 15 milliseconds, the actual effect is 2 in 10 milliseconds.

【Configuration Example]】1: Configure the sending rate of ICMP destination unreachable packets triggered by the unfragmentable bit in the IP header to be 100 per second.

```
AC-FS(config)# ip icmp error-interval DF 1000 100
```

2: Configure the sending rate of other ICMP error packets to be 10 per second.

```
AC-FS(config)# ip icmp error-interval 1000 10
```

【Verification】Use show running-config to view the configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.7 ip icmp timestamp

Configure the timestamp query function.

ip icmp timestamp

Unconfigure the timestamp query function.

no ip icmp timestamp

【Parameter Description】-

【Default Configuration】 The timestamp query function is enabled by default.

【Command Mode】 Global mode

【Default Level】 2

【Usage Guide】

【Configuration Example]】1: The configuration disables the timestamp query function.

AC-FS(config)# no ip icmp timestamp

```
AC-FS#show running-config | include ip icmp timestamp
no ip icmp timestamp
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.8 ip directed-broadcast

Enables the translation of IP directed broadcasts to physical broadcasts.

ip directed-broadcast [access-list-number]

Cancel the conversion of directed broadcasts to physical broadcasts.

no ip directed-broadcast

【Parameter Description】

Parameter	Description
access-list-number	(Optional) Access list number, in the range from 1 to 199 and from 1300 to 2699. After an access list number has been defined, only the IP directed broadcast packets that match this access list are converted.

【Default Configuration】Close

【Command Mode】 Interface mode

【Default Level】 2

【Usage Guide】 IP directed broadcast packet is an IP packet whose destination address is an IP subnet broadcast address. For example, the packet with the destination address 172.16.16.255 is called a directed broadcast packet. However, the node that generates this packet is not a member of the destination subnet.

The device that is not directly connected to the destination subnet receives an IP directed broadcast packet and handles this packet in the same way as forwarding a unicast packet. After the directed broadcast packet reaches a device that is directly connected to this subnet, the device converts the directed broadcast packet into a flooding broadcast packet (typically the broadcast packet whose destination IP address is all "1"), and then sends the packet to all the hosts in the destination subnet in themanner of link layer broadcast.

You can enable conversion from directed broadcast into physical broadcast on a specified interface, so that this interface can forward a direct broadcast packet to a directly connected network. This command affects only the final transmission of directed broadcast packets that have reached the destination subnet instead of normal forwarding of other directed broadcast packets.

You can also define an access list on an interface to control which directed broadcast packets to forward. After an access list is defined, only the packets that conform to the conditions defined in the access list undergo conversion from directed broadcast into physical broadcast.

If the no ip directed-broadcast command is configured on an interface, FSOS will discard the directed broadcast packets received from the directly connected network.

【Configuration Example】 The following example enables forwarding of directed broadcast packet on the fastEthernet 0/1 .

```
AC-FS(config)# interface gigabitEthernet 0/1
AC-FS(config-if-GigabitEthernet 0/1)# ip directed-broadcast
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.9 ip local pool

Create an IP address pool.

ip local pool pool-name low-ip-address [high-ip-address]

Delete an IP address pool.

no ip local pool pool-name [low-ip-address [high-ip-address]]

【Parameter Description】

Parameter	Description
pool-name	Specifies the name of the local IP address pool, default is the default address pool name
low-ip-address	The smallest IP address in the IP address pool
high-ip-addres	Optional, the largest IP address in the IP address pool. If no maximum IP address is specified, the IP address

【Default Configuration】 No IP address pool is configured by default.

【Command Mode】 Global configuration mode

【Default Level】 2

【Usage Guide】 You can use this command to create one or more IP address pools for PPP to assign IP addresses to connected users.

【Configuration Example】 1: Create a local IP address pool with the name quark and the IP address range from 172.16.23.0 to 172.16.23.255.

```
AC-FS(config)#ip local pool quark 172.16.23.0 172.16.23.255
```

【Verification】 Use show ip pool to view the created address pool.

【Prompt Information】 2. It is not allowed to create an ip address pool without enabling the address pool function. If it is created, it will prompt:

% IP local pool is disabled!

3. If high-ip-address is less than low-ip-address, or high-ip-address and low-ip-address are not in the same network segment,

Then prompt:

% Invalid address range!

【Common Mistake】 4. The configured high-ip-address is smaller than the low-ip-address.

5. The configured high-ip-address and low-ip-address are not in the same network segment.

【Platform Description】-

1.10 ip mask-reply

Enable ICMP mask reply message.

ip mask-reply

Turn off ICMP mask reply messages.

no ip mask-reply

【Parameter Description】 -

【Default Configuration】 Enable sending ICMP mask response message by default

【Command Mode】 Interface mode

【Default Level】 2

【Usage Guide】 Network devices sometimes need to know the subnet mask of a subnet on the Internet. In order to obtain this information, the network device can send an ICMP mask request message, and the network device that receives the ICMP mask request message will send the mask reply message.

【Configuration Example】1: The gigabitEthernet 0/1 interface of the device will respond to the ICMP mask request message.

```
AC-FS(config)# interface gigabitEthernet 0/1
AC-FS(config-if-GigabitEthernet 0/1)# ip mask-reply
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.11 ip mtu

Configure the IP packet maximum transmission unit (MTU).

ip mtu bytes

Restore Default Configuration.

no ip mtu

【Parameter Description】

Parameter	Description
Bytes	Maximum transmission unit of IP packet, in the range from 68 to 1500.

【Default Configuration】 The default value is the same as the value configured by the interface command mtu.

【Command Mode】 Interface mode

【Default Level】 2

【Usage Guide】 If an IP packet exceeds the IP MTU size, the RGOS software will split the packet. All devices on the same physical network segment must have the same IP MTU of their interconnected interfaces.

If you use the interface configuration command mtu to set the maximum transmission unit value of the interface, the IP MTU value will be automatically consistent with the MTU value of the interface. Conversely, if the IP MTU value is adjusted, the MTU value of the interface will not change accordingly.

【Configuration Example】 The following iexample sets the IP MTU value of the fastEthernet 0/1 interface to 512 bytes..

```
AC-FS(config)# interface gigabitEthernet 0/1
AC-FS(config-if-GigabitEthernet 0/1)# ip mtu 512
```

【Verification】1: show ip interface gi 0/1 shows that the IP interface MTU is: 512.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.12 ip redirects

Enable ICMP redirect messages.

ip redirects

Turn off ICMP redirection.

no ip redirects

【Parameter Description】 -

【Default Configuration】 It is enabled by default.

【Command Mode】 Interface mode

【Default Level】 2

【Usage Guide】 When the route is not optimal, it is possible that the data packets received by the device from an interface are also sent out from the interface. If the device resends the packet from the receiving interface, the device sends an ICMP redirect message to the data source, telling the data source that the gateway to the destination address is another device on the same subnet. In this way, the data source will send subsequent data packets according to the best path.

The FSOS software enables ICMP redirection by default.

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.13 ip source-route

Enable the processing of IP source routing information.

ip source-route

Disables the processing of IP source routing information.

no ip source-route

【Parameter Description】 -

【Default Configuration】 Default enabled

【Command Mode】 Global mode

【Default Level】 2

【Usage Guide】 FSOS supports IP source routing. When the device receives an IP packet, it checks the IP header for options such as strict source routing, loose source routing, record routing, etc. These options are described in detail in RFC 791. If it is detected that the packet has one of the options enabled, the corresponding action will be performed; if an invalid option is detected, an ICMP Parameter problem message will be sent to the data source, and the packet will be discarded.

The FSOS software supports IP source routing by default.

【Configuration Example】 The following example disables the IP source route.

```
AC-FS(config)# no ip source-route
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.14 ip ttl

Configure the TTL value of unicast packets sent by the local machine.

ip ttl value

Unconfigure the TTL value of unicast packets sent by the local machine.

no ip ttl

【Parameter Description】

Parameter	Description
value	Sets the TTL value of the unicast packet, in the range from 0 to 255.

【Default Configuration】 The default value is 64.

【Command Mode】 Global mode

【Default Level】 2

【Usage Guide】 -

【Configuration Example】 The following example sets the TTL value of the unicast packet to 100.

```
AC-FS(config)# ip ttl 100
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.15 1.15ip ttl-expires enable

Configure the machine to send TTL timeout messages.

ip ttl-expires enable

Unconfigure the machine to send TTL timeout messages.

no ip ttl-expires enable

【Parameter Description】-

【Default Configuration】 The function of sending TTL timeout message is enabled by default.

【Command Mode】 Global mode

【Default Level】 2

【Usage Guide】 -

【Configuration Example】1: Configure to disable the function of sending TTL time-out messages by this machine.

```
AC-FS(config)# no ip ttl-expires enable
```

```
AC-FS#show running-config | include ip ttl-expires enable
no ip ttl-expires enable
```

【Verification】

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

1.16 ip unnumbered

Configure the interface to borrow an IP address.

ip unnumbered interface-type interface-number

Cancel this configuration.

no ip unnumbered

【Parameter Description】

Parameter	Description

interface-type	Type of the associated interface.
interface-number	No. of the associated interface.

【Default Configuration】 By default, no numbered interface is configured.

【Command Mode】 Interface mode

【Default Level】 2

【Usage Guide】 An unnumbered interface means that only the IP protocol is enabled on the interface, but no IP address is assigned. An unnumbered interface needs to be associated with an interface with an IP address. An IP packet generated by an unnumbered interface whose source IP address is the IP address of the associated interface. In addition, the routing protocol process also decides whether to send routing update packets to the unnumbered interface according to the IP address of the associated interface. When using an unnumbered interface, you need to pay attention to the following restrictions:

6. The Ethernet interface cannot be configured as an unnumbered interface.

7. When the serial port is encapsulated with SLIP, HDLC, PPP, LAPB, and Frame-relay, it can be configured as an unnumbered interface. However, when frame relay is encapsulated, only point-to-point subinterfaces are allowed to configure unnumbered interfaces. X.25 encapsulation does not allow configuration of unnumbered interfaces.

8. The ping command cannot be used to detect whether the unnumbered interface is working properly, because the unnumbered interface has no IP address. However, the status of unnumbered interfaces can be monitored remotely through SNMP.

9. Cannot network boot through unnumbered interface.

【Configuration Example】 1: The configuration interface is configured as an unnumbered interface, and the associated interface is gigabitEthernet 0/1.

```
AC-FS(config)# int virtual-ppp 1
AC-FS(config-if-Virtual-ppp 1)# ip unnumbered gigabitEthernet 0/1
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.17 ip unreachables

Enable ICMP protocol unreachable messages.

ip unreachables

Turn off sending ICMP protocol unreachable messages.

no ip unreachables

【Parameter Description】 -

【Default Configuration】 Default enabled

【Command Mode】 Interface mode

【Default Level】 2

【Usage Guide】 If the FSOS software receives a unicast message whose destination address is itself, and cannot process the upper-layer protocol of the message, it will send an ICMP

Destination unreachable message.

If the FSOS software cannot forward a packet because there is no routing, it sends an ICMP host unreachable message to the data source.

This command affects all ICMP target unreachable messages.

【Configuration Example】 1: Disable gigabitEthernet 0/1 interface to send ICMP target unreachable message.

```
AC-FS(config)# interface gigabitEthernet 0/1
AC-FS(config-if-GigabitEthernet 0/1)# no ip unreachables
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.18 peer default ip address

Assign an IP address to the peer for PPP negotiation.

peer default ip address {ip-address | pool [pool-name] }

Unassign the IP address to the peer.

no peer default ip address

【Parameter Description】

Parameter	Description
ip-address	Allocates an IP address to the peer end.
pool-name	(Optional) Specifies the address pool name. If not specified, the default address pool is used.

【Default Configuration】 By default, the interface does not assign an IP address to the peer.

【Command Mode】 Interface mode

【Default Level】 2

【Usage Guide】 When the peer interface has not been configured with an IP address but the local device already has an IP address, you can configure the local device to assign an IP address to the peer interface. In this case, you need to configure the ip address negotiate command on the peer device and the peer default ip address command on the local device, so that the peer interface accepts the IP address assigned by PPP negotiation.

This command only supports configuration on point-to-point interfaces encapsulating PPP or SLIP protocols.

The peer default ip address pool command allocates an IP address to the peer from the IP address pool. This IP address pool is the address pool configured by the ip local pool command.

The peer default ip address ip-address command directly assigns an IP address to the peer. This command cannot be configured on virtual template interfaces and asynchronous interfaces.

【Configuration Example】 The following example enables interface dialer 1 to allocate IP address 10.0.0.1 to the peer end.

```
AC-FS(config)# interface dialer 1
AC-FS(config-if-dialer 1)# peer default ip address 10.0.0.1
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】-

【Platform Description】-

1.19 show ip interface

Use this command to display the IP status information of an interface.

show ip interface [interface-typeinterface-number| brief]

【Parameter Description】

Parameter	Description
interface-type	Specifies interface type.
interface-number	Specifies interface number.
brief	Displays the brief configurations about the IP of the layer-3 interface (including the interface primary ip, secondary ip and interface status)

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】 When an interface is available, RGOS will create a direct route in the routing table. The available interface refers to the interface through which the RGOS software can send and receive data packets. If an interface changes from an available state to an unavailable state, the RGOS software will delete the corresponding directly connected route from the routing table. The line protocol status will show "UP" if the interface is up, i.e. allowing two-way communication; if only the physical line is up, the interface status will show "UP". Different interface types may display different results because some of the contents are options specific to certain interfaces.

【Configuration Example】1: Display IP status information of all interfaces.

```
AC-FS#show ip interface brief
Interface            IP-Address(Pri)   IP-Address(Sec) Status Protocol
GigabitEthernet 0/10  2.2.2.2/24.....3.3.3.3/24   down   down
GigabitEthernet 0/11  no address      no address     down     down
VLAN 1                   1.1.1.1/24      no address     down     down
```

Status Describes the link status of the interface. The values are up, down, and administratively down (the user runs the shutdown command to force the interface to shut down).

Protocol Description The IPv4 protocol status of the interface.

2: Display the IP status information of the VLAN 1 interface.

```
AC-FS#show ip interface vlan 1
VLAN 1
  IP interface state is: DOWN
  IP interface type is: BROADCAST
  IP interface MTU is: 1500
  IP address is:
    1.1.1.1/24 (primary)
  IP address negotiate is: OFF
  Forward direct-broadcast is: OFF
  ICMP mask reply is: ON
  Send ICMP redirect is: ON
  Send ICMP unreachabled is: ON
  Proxy ARP is: OFF
ARP packet input number:           0
     Request packet:                 0
     Reply packet:                   0
     Unknown packet:                0
TTL invalid packet number:          0
ICMP packet input number:          0
     Echo request:                   0
Echo reply:                       0
     Unreachable:                    0
     Source quench:                  0
     Routing redirect:                 0
```

Description of Fields:

Field	Description
IP interface state is:	The network interface is available and its interface hardware state and line protocol state are both.
IP interface type is:	"UP".
IP interface MTU is:	Displays the interface type, such as broadcast, point-to-point, etc.
IP address is:	Displays the MTU value set by the interface.
IP addre s negotiate is:	Displays interface IP address and mask information.
Forward direct-boardcast is:	Displays whether the interface IP address is obtained through negotiation.
ICMP mask reply is:	Displays whether to forward directed broadcasts.
Send ICMP redirect is:	Displays whether to send ICMP mask response packets.
Send ICMP unreachabled is:	Displays whether to send ICMP redirect packets.
Proxy ARP is:	Displays whether to send ICMP unreachable packets.

ARP packet input number: 0 Request packet: 0 Reply packet: 0 Unknown packet: 0	Displays the total number of ARP packets received on the interface, including: ARP request message ARP reply message Unknown type of message
TTL invalid packet number:	Displays the number of invalid TTL packets received on the interface
ICMP packet input number: 0 Echo request: 0 Echo reply: 0 Unreachable: 0 Source quench: 0 Routing redirect: 0	Displays the total number of ICMP packets received on the interface, including the following packets: Echo Request Packet Echo Reply Packet Unreachable Packet The source station suppresses packets Route redirect message

【Prompt Information】-

【Platform Description】-

1.20 show ip packet queue

Display protocol stack IP packet sending and receiving statistics.

show ip packet queue

【Parameter Description】 -

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】-

【Configuration Example】

【Configuration Example】

```
AC-FS#show  ip packet  queue
Receive 31925 packets(fragment=0):
  IP packet receive queue: length 0, max 1542, overflow 0.
  Receive 13 ICMP echo packets, 25 ICMP reply packets .
  Discards:
    Failed to alloc skb: 0.
    Receive queue overflow: 0.
    Unknow protocol drops: 0.
    ICMP rcv drops: 0. for skb check fail.
    ICMP rcv drops: 0. for skb is broadcast.
Sent packets:
  Success: 15644
  Generate 13 and send 8 ICMP reply packets, send 26 ICMP echo packets.
  It records 187 us as max time in ICMP reply process.
  Failed to alloc efbuf: 0
  Dropped by EFMP: 0
  NoRoutes: 887
  Get vrf fails: 0
  Cannot assigned address drops: 0
  Failed to encapsulate ethernet head: 0
ICMP error queue: length 0, max 1542, overflow 0.
```

Field	Description
IP packet receive queue	Protocol stack IP receive queue Parameter.
Discards	Packets discarded during reception.
Sent packets	Statistics of sent IP packets.
ICMP error queue	ICMP error message receiving queue Parameter.

【Prompt Information】-

【Platform Description】-

1.21 show ip packet statistics

View statistics about IP packets.

show ip packet statistics [total | interface-name]

【Parameter Description】

Parameter	Description
interface-name	Interface name.
total	Displays the total statistics of all interfaces.

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】-

【Configuration Example】 The following example displays the output of this command.

```
FS#show ip packet statistics
Total
  Received 113962 packets, 11948991 bytes
    Unicast:90962,Multicast:5232,Broadcast:17768
    Discards:0
      HdrErrors:0(BadChecksum:0,TTLExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 34917 packets, 1863146 bytes
```

```
    Unicast:30678,Multicast:4239,Broadcast:0
GigabitEthernet 0/1
  Received 6715 packets, 416587 bytes
    Unicast:2482,Multicast:4233,Broadcast:0
    Discards:0
      HdrErrors:0(BadChecksum:0,TTLExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 6720 packets, 417096 bytes
    Unicast:2481,Multicast:4239,Broadcast:0
Loopback 0
  Received 0 packets, 0 bytes
    Unicast:0,Multicast:0,Broadcast:0
    Discards:0
      HdrErrors:0(BadChecksum:0,TTLExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 0 packets, 0 bytes
    Unicast:0,Multicast:0,Broadcast:0
Tunnel 1
  Received 0 packets, 0 bytes
    Unicast:0,Multicast:0,Broadcast:0
    Discards:0
      HdrErrors:0(BadChecksum:0,TTLExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 21584 packets, 1122848 bytes
    Unicast:21584,Multicast:0,Broadcast:0
```

Field	Description
Total	Indicates that what is displayed next is the sum of the statistics of all interfaces.
GigabitEthernet 0/1	Indicates that the next display is the statistical value information for this specific interface.
Received	Number of packets received, in bytes. And unicast/multicast/broadcast statistics, including the number of lost packets, and the corresponding packet loss reasons.
Sent	The number of packets sent, the number of bytes, the number of unicast/multicast/broadcast.

【Prompt Information】-

【Platform Description】-

1.22 show ip pool

View the system's IP address pool information.

show ip pool [pool-name]

【Parameter Description】

Parameter	Description
pool-name	Specifies the IP address pool.

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】-

【Configuration Example】 The following example displays all IP address ranges.

```
FS# show ip pool
FS(config)#show ip pool
Pool   Begin                End                Free        In use
default      1.1.1.1        1.1.1.1            1           0
pool1 2.2.2.2               2.2.2.254          253         0
pool2 3.1.1.1               3.2.1.1            65537       0
pool3 192.168.1.1           192.168.1.254
```

【Field Description】

Field	Description
Pool	Address pool name
Begin	The start IP address of the address pool
Free	The number of free IP addresses in the address pool
In use	The number of IP addresses in use in the address pool

【Prompt Information】 10. If no address pool is created, it will display:

No IP local pools exist

【Platform Description】-

1.23 show ip raw-socket

Show all IPv4 raw sockets.

show ip raw-socket [num]

【Parameter Description】

Parameter	Description
num	Protocol.

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】-

【Configuration Example】 The following example displays all IPv4 raw sockets.

```
AC-FS# show  ip  raw-socket
Number  Protocol   Process   name
1       ICMP  dhcp.elf
2       ICMP     vrrp.elf
3       IGMP     igmp.elf
4       VRRP        vrrp.elf
Total: 4
```

【Field Description】

Field	Description
Number	Number.
Protocol	Protocol.
Process name	Process name.
Total	Total number.

【Prompt Information】-

【Platform Description】-

1.24 show ip sockets

Display all IPv4 sockets, you can know which UDP ports and TCP ports provide services to the outside world.

show ip sockets

【Parameter Description】 = -

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】-

【Configuration Example】 The following displays all IPv4 sockets..

```
AC-FS# show ip sockets
Number Process name     Type     Protocol LocalIP:Port  ForeignIP:Port          State
1      dhcp.elf         RAW      ICMP     0.0.0.0:1.....0.0.0.0:0              *
2      vrrp.elf         RAW      ICMP     0.0.0.0:1      0.0.0.0:0             *
3      igmp.elf         RAW      IGMP     0.0.0.0:2      0.0.0.0:0             *
4      vrrp.elf         RAW      VRRP     0.0.0.0:112    0.0.0.0:0             *
5      dhcpc.elf        DGRAM    UDP      0.0.0.0:68     0.0.0.0:0             *
6      rg-snmpd         DGRAM    UDP      0.0.0.0:161    0.0.0.0:0             *
7      wbav2            DGRAM    UDP      0.0.0.0:2000   0.0.0.0:0             *
8      vrrp_plus.elf    DGRAM    UDP      0.0.0.0:3333   0.0.0.0:0             *
9      mpls.elf         DGRAM    UDP      0.0.0.0:3503   0.0.0.0:0             *
10     rds_other_th     DGRAM    UDP      0.0.0.0:3799   0.0.0.0:0             *
11     rg-snmpd         DGRAM    UDP      0.0.0.0:14800  0.0.0.0:0             *
12     rg-sshd          STREAM   TCP      0.0.0.0:22     0.0.0.0:0             LISTEN
13     rg-telnetd       STREAM   TCP      0.0.0.0:23     0.0.0.0:0             LISTEN
14     wbard            STREAM   TCP      0.0.0.0:4389   0.0.0.0:0             LISTEN
15     wbard            STREAM   TCP      0.0.0.0:7165   0.0.0.0:0             LISTEN
Total: 15
```

【Field Description】

Field	escription
Number	Serial number.
Process name	Process name.
Type	Socket type, including the following types: RAW: raw sockets DGRAM: datagram type

	STREAM: stream type.
Protocol	Protocol.
LocalIP:Port	Local IP address and port.
ForeignIP:Port	Peer IP address and port.
State	State. This field is for only TCP sockets.
Total	The total number of sockets.

【Prompt Information】-

【Platform Description】-

1.25 show ip udp

Display all IPv4 UDP sockets, you can know which UDP ports provide services to the outside world.

show ip udp [local-port num]

Displays statistics for IPv4 UDP sockets.

show ip udp statistics

【Parameter Description】

Parameter	Description
local-portnum	Local port number.

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】-

【Configuration Example】 The following example displays all IPv4 UDP sockets.

```
AC-FS# show ip udp
Number Local Address          Peer Address          Process      name
1      0.0.0.0:68.....0.0.0.0:0             dhcpc.elf
2      0.0.0.0:161            0.0.0.0:0             rg-snmpd
3      0.0.0.0:2000           0.0.0.0:0             wbav2
4      0.0.0.0:3333           0.0.0.0:0             vrrp_plus.elf
5      0.0.0.0:3503           0.0.0.0:0             mpls.elf
6      0.0.0.0:3799           0.0.0.0:0             rds_other_th
7      0.0.0.0:14800          0.0.0.0:0             rg-snmpd
```

【Field Description】

Field	Description
Number	Number.
Local Address	Local IP address and port.
Peer Address	Peer IP address and port.
Process name	Process name.

【Prompt Information】-

【Platform Description】-

2 ARP

2.1 arp

Configure static ARP.

arp ip-address mac-address type

Cancel static ARP.

no arp ip-address

【Parameter Description】

Parameter	Description
ip-address	The IP address corresponding to the MAC address is divided into four groups of cimal values, and the groups are separated by dots.
mac-address	Data link layer address, composed of 48 bits.
type	ARP encapsulation type. For Ethernet interfaces, the keyword is arpa.

【Default Configuration】 There is no static mapping record in the ARP buffer table.

【Command Mode】 Global mode

【Default Level】 2

【Usage Guide】FSOS uses the ARP buffer table to find the 48-bit MAC address based on the 32-bit IP address.

Since most hosts support dynamic ARP resolution, it is usually not necessary to configure static ARP mapping. Use the clear arp-cache command to delete dynamically learned ARP mappings.

【Configuration Example】 1: Configure ARP static mapping records for hosts on the Ethernet.

```
AC-FS(config)# arp 1.1.1.1 4e54.3800.0002 arpa
```

【Verification】1: The show arp command shows the corresponding static entries generated.

【Prompt Information】1: The VRF named xyz does not exist or address-family ipv4 is not enabled, resulting in the failure to add or delete static ARP.

```
% ARP:vrf xyz does not exist. Create first.

% ARP:vrf xyz ipv4 address-family is not enable. Enable first.
```

2: The ARP entry does not exist or the entry is reserved, resulting in the failure of static ARP deletion.

Cannot remove ARP. ARP entry does not exist or reserved.

3: The static ARP entry fails to be added, usually because the ARP cache table is full, or the corresponding IP address is the local address.

Cannot add static ARP.

【Common Mistake】-

【Platform Description】-

2.2 arp any-ip

Enable ARP learning function.

arp-learning enable

Disable the ARP learning function.

no arp-learning enable

【Parameter Description】 -

【Default Configuration】 By default, the dynamic ARP learning function is enabled on the interface.

【Command Mode】 Interface configuration mode

【Default Level】 2

【Usage Guide】 If it is confirmed that the device has learned the dynamic ARP entries that need to be learned, after converting the dynamic ARP to static ARP through the web, it is recommended to enable this function, otherwise it is not recommended to enable this function. After the dynamic ARP non-learning function is enabled, if there is a dynamic ARP entry, if the user needs to convert the dynamic ARP entry into a static ARP entry, it can be configured through the web. If the user needs to clear the dynamic ARP entry, a certain Users can use the clear arp command to access the Internet. Otherwise, the dynamic ARP entry will be aged normally. After the aging time

expires, the dynamic ARP entry will be cleared. After enabling the interface to stop the dynamic ARP learning function, the AnyIP function and the ARP trusted detection function become invalid.

【Configuration Example】 1: Enable dynamic ARP learning function.

```
AC-FS(config)# interface gi 0/0
AC-FS(config-if-GigabitEthernet 0/0)# arp-learning enable
```

2: Disable the dynamic ARP learning function.

```
AC-FS(config)# interface gi 0/0
AC-FS(config-if-GigabitEthernet 0/0)# no arp-learning enable
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

2.3 arp any-ip

Enable any IP ARP function.

arp any-ip

Disable any IP ARP function.

no arp any-ip

【Parameter Description】 -

【Default Configuration】 This function is disabled by default.

【Command Mode】 Interface mode

【Default Level】 2

【Usage Guide】 In the following two cases, the user must modify the configuration to access the Internet:

11. The user IP address belongs to the network segment of the interface directly connected to the device, but the configured gateway IP address is not the IP address configured on the interface directly connected to the device.

12. The user IP address does not belong to the network segment of the interface directly connected to the device, but belongs to the network segment of other interfaces of the device, that is, there is a conflict.

Since the user IP address does not belong to the network segment directly connected to the device, the generation of the dynamic ARP entry and the direct route depends on the user to initiate an ARP request first. Therefore, the following scenarios (but not limited to the following scenarios) will cause the user to be unable to access the Internet. , the client needs to clear the ARP entry and then relearn the gateway address:

13. The device proxy responds to the ARP request. After the user learns the MAC address of the device, it clears the dynamic ARP entry on the device, causing the user to dynamically

ARP entries and directly connected routes are deleted, and response packets cannot reach the client.

14. The device proxy responds to the ARP request. After the user learns the MAC address of the device, disable the any IP ARP function on the interface, and then enable it again.

If the any IP ARP function is disabled on the interface, the dynamic ARP entries and direct routes of the user will be deleted, so that the response packets cannot reach the user end.

If there is a corresponding static ARP entry or an ARP entry for the VRRP IP address, the dynamic ARP entry generated by any IP ARP will fail to be added or be overwritten, and the any IP ARP function will not take effect.

【Configuration Example】 1: Enable any IP ARP function.

```
AC-FS(config)# interface gi 0/0
AC-FS(config-if-GigabitEthernet 0/0)# arp any-ip
```

2: Disable any IPARP function.

```
AC-FS(config)# interface gi 0/0
AC-FS(config-if-GigabitEthernet 0/0)# no arp any-ip
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

2.4 arp cache interface-limit

Configure to limit the number of ARP learning on an interface.

arp cache interface-limit limit

Restore Default Configuration.

no arp cache interface-limit

【Parameter Description】

Parameter	Description
limit	Sets the maximum number of ARP learned on the interface, including static and dynamic ARPs, in the range from 0 to the number supported on the interface. 0 indicates that the number is not limited.

【Default Configuration】 By default, the number of ARP learning on the interface is not limited.

【Command Mode】 Interface configuration mode

【Default Level】 2

【Usage Guide】 Limiting the number of ARP learning on an interface can prevent malicious ARP attacks and allow the device to generate a large number of ARP entries, occupying too many entry resources. The configured value must not be less than the number of ARP entries that the current interface has learned, otherwise the configuration will not take effect. This limit is limited by the ARP capacity supported by the device.

【Configuration Example】 1: Configure to limit the number of interface ARP learning to 300.

```
AC-FS(config)# interface gi 0/0
AC-FS(config-if-GigabitEthernet 0/0)# arp cache interface-limit 300
```

2: Disable to limit the number of ARP learning on the interface.

```
AC-FS(config)# interface gi 0/0
AC-FS(config-if-GigabitEthernet 0/0)# no arp cache interface-limit
```

【Verification】 show running-config Check whether the relevant configuration takes effect.

【Prompt Information】 -

【Common Mistake】-

【Platform Description】-

2.5 arp gratuitous-send interval

Configure to send gratuitous ARP requests periodically.

arp gratuitous-send interval seconds [number]

Disable timing to send gratuitous ARP requests.

no arp gratuitous-send

【Parameter Description】

Parameter	Description
seconds	The interval for sending gratuitous ARP requests, in seconds, in the range of <1-3600>.
number	The number of gratuitous ARP requests sent, the default value is 1, the value range is <1-100>.

【Default Configuration】 The function of periodically sending gratuitous ARP requests is not enabled on the interface.

【Command Mode】 Interface mode

【Default Level】 2

【Usage Guide】When the network interface of the device is used as the gateway of the downlink device, if the downlink device acts as a gateway, you can configure this interface to send gratuitous ARP requests periodically to announce that it is the real gateway.

【Configuration Example】 1. The following example sets to send one free ARP request to SVI 1 per second.

```
AC-FS(config)# interface vlan 1
AC-FS(config-if)# arp gratuitous-send interval 1 1
```

2: Cancel the scheduled sending of gratuitous ARP requests to interface VLAN 1.

```
AC-FS(config)# interface vlan 1
AC-FS(config-if)# no arp gratuitous-send
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.6 arp proxy-resolved

Configure the VRRP host to proxy the user's response only when the destination IP has been resolved when it does the local ARP proxy response.

arp proxy-resolved

When a VRRP host responds with an ARP proxy, it does not need to judge the existence of the ARP of the destination IP.

no arp proxy-resolved

【Parameter Description】-

【Default Configuration】 Open by default.

【Command Mode】 Global mode

【Default Level】 2

【Usage Guide】Configure arp proxy-resolved, when the VRRP master device receives an ARP request, it will first determine whether the ARP of the destination IP exists when proxying: if it exists, it will proxy; otherwise, it will not respond by proxy, and the gateway will actively open up the destination IP ARP (that is, the gateway will actively broadcast the ARP request for the destination IP) to prevent the gateway from being unable to proxy the ARP request of the destination IP because the gateway does not have the ARP of the destination IP.

Configure no arp proxy-resolved. When the VRRP master device receives an ARP request, if it meets the proxy conditions, it will directly proxy it without judging whether the ARP of the destination IP has been resolved.

【Configuration Example]】1: Disable VRRP The host needs to first determine the ARP existence of the destination IP when proxying the ARP reply.

```
AC-FS(config)# no arp proxy-resolved
```

【Verification】show running-config Check whether the relevant configuration takes effect.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.7 arp resolve vlan

Configure ARP to actively send broadcast resolution requests to specific Subvlans in the Supervlan.

arp resolve vlan {vlan-list | none}

Delete ARP to actively send broadcast resolution requests to specific Subvlans in Supervlan.

no arp resolve vlan {vlan-list | none}

Restore Default Configuration.

default arp resolve vlan

【Parameter Description】

Parameter	Description
vlan-list	ARP actively sends broadcast resolution requests to Vlans in the vlan-list in Supervlan. After configuration, ARP only sends ARP broadcasts to these Vlan lists.
none	Do not send ARP broadcast requests to any Subvlan in the Supervlan.

【Default Configuration】 It is closed by default.

【Command Mode】 Global mode

【Default Level】 2

【Usage Guide】 If there are many Subvlans in a Supervlan, when the device actively performs ARP broadcast analysis, it will send ARP broadcast requests to the entire Supervlan by default. Because there are too many Subvlans, a large number of packets need to be copied, which affects the performance of the device.

For most users (such as PCs or servers), the ARP of the gateway will be requested before accessing the network, so there is no need to actively broadcast ARP to the Subvlan where such users are located. For dumb terminal type users (not actively sending gratuitous ARP), it can be deployed in the vlan-list specified by arp resolve vlan vlan-list. At this time, the device will actively resolve ARP to these Vlans.

After configuring arp resolve vlan vlan-list, the device only sends ARP broadcast requests to the VLANs specified in the vlan-list in the Supervlan, and other Subvlans that are not in the vlan-list will not actively send ARP broadcast requests. In particular, if an authentication-free vlan is configured, and the authentication-free vlan is not in the vlan-list list of arp resolve vlan, it will no longer actively broadcast ARP to the authentication-free vlan!

【Configuration Example]】 1: Configure the device to actively resolve the Vlan as 10-20, 25-30.

```
AC-FS(config)# arp resolve vlan 10-20, 25-30
```

2: Delete the device that actively resolves Vlan10-20.

```
AC-FS(config)# no arp resolve vlan 10-20

3: Configure the device not to actively resolve ARP
to any Subvlan of the Supervlan

AC-FS(config)# arp resolve vlan none
```

【Verification】 show running-config Check whether the relevant configuration takes effect.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

2.8 arp retry interval

Configure the interval for retransmitting ARP requests.

arp retry interval seconds

Restore Default Configuration.

no arp retry interval

【Parameter Description】

Parameter	Description
seconds	The retransmission time of ARP request can be set from 1 to 3600 seconds, and the default value is 1 second.

【Default Configuration】 ARP request retransmission interval is 1 second.

【Command Mode】 Global mode

【Default Level】 2

【Usage Guide】 When it is found that the device frequently sends out ARP requests, causing other problems such as network busyness, you can set the retransmission time of ARP requests to be longer, generally not exceeding the aging time of dynamic ARP entries.

【Configuration Example】 The following example sets the retry interval of the ARP request as 30 seconds.

```
AC-FS(config)# arp retry interval 30
```

【Related Command】

Command	Description
arp retry times	Number of times for retransmitting an ARP request message.

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

2.9 arp retry times

Configure the number of times to retransmit arp request packets.

arp retry times number

Restore Default Configuration.

no arp retry times\

【Parameter Description】

Parameter	Description
number	The number of times the same ARP request is sent, range <1-100>. When set to 1, it means that the ARP request will not be retransmitted, but only one ARP request message will be sent.

【Default Configuration】 If no ARP reply message is received, the ARP request message will be sent 5 times and then time out.

【Command Mode】 Global mode.

【Default Level】 2

【Usage Guide】 When it is found that the device frequently sends out ARP requests, causing other problems such as network busyness, you can set the number of retransmissions of ARP requests to a smaller value. Generally, do not set the number of retransmissions too large.

【Configuration Examples】1: Configure local ARP requests not to be retransmitted.

```
AC-FS(config)# arp retry times 1
```

2: Configure the local ARP request to retransmit once.

```
AC-FS(config)# arp retry times 2
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.10 arp scan

Enable ARP scanning.

arp scan [start-ip-address end-ip-address]

【Parameter Description】

Parameter	Description
start-ip-address	The starting IP address of the ARP scan interval. The starting IP address must be less than or equal to the ending IP address.
end-ip-address	The ending IP address of the ARP scan interval. The ending IP address must be greater than or equal to the starting IP address.

【Default Configuration】 This function is disabled by default.

【Command Mode】 Interface configuration mode.

【Default Level】 2

【Usage Guide】 1. The ARP scanning function is generally used in combination with the function of WEB dynamic ARP to static ARP.

2. Do not scan the IP of the existing neighbor ARP entry.

3. If the user knows the IP address range allocated by neighbors in the LAN, he can scan the neighbors in the range by specifying the ARP scan interval to reduce the scanning waiting time. The number of hosts specified in the ARP scan interval must be less than or equal to 1024.

4. The starting IP address and ending IP address of the ARP scanning range must be in the same network segment as the IP address (primary IP address or secondary IP address) of the interface.

5. If the user does not specify the starting IP address and ending IP address of the ARP scanning range, only the neighbors in the main IP address network segment under the interface will be scanned. And the network segment mask of the primary IP address must be greater than or equal to 22 bits.

6. ARP scanning belongs to ready-to-use, configure once, take effect once, does not support configuration save and take effect next time.

7. ARP scan time point: Execute once during configuration. The execution condition is that the interface is up at Layer 3 (that is, the link is up and an IP address is configured).

【Configuration Example】1: Configure ARP scanning function, do not specify IP address range.

```
AC-FS(config)# interface gi 0/0
AC-FS(config-if-GigabitEthernet 0/0)# arp scan
```

2: Configure the ARP scanning function and specify the IP address range.

```
AC-FS(config)# interface gi 0/0
AC-FS(config-if-GigabitEthernet 0/0)# arp scan 1.1.1.1 1.1.1.10
```

【Verification】-

【Prompt Information】 1. start-ip-address or end-ip-address is not a valid host address, or start-ip-address is greater than end-ip-address, or start-ip-address and end-ip-address and interface If the ip address is not on the same network segment, it will prompt:

%notice: Invalid ip address range.

2. If the number of hosts in the specified range is greater than 1024, print:

%notice: Failed to scan because ip address range is larger than 1024.

3. If the interface does not have Layer 3 up, it will prompt:

%notice: Failed to scan because this interface is not up.

【Common Mistake】 1. The start-ip-address is greater than the end-ip-address.

2. The start-ip-address and end-ip-address are not on the same network segment as the ip address of the interface.

【Platform Description】 This command is only supported on egress gateway devices such as EG, NPE, and NBR.

2.11 arp suppress-auth-vlan-req

Enable the function of suppressing the sending of ARP requests to the authentication VLAN on the SVI interface.

arp suppress-auth-vlan-req

Disable the function of suppressing the sending of ARP requests to the authentication VLAN on the SVI interface.

no arp suppress-auth-vlan-req

【Parameter Description】-

【Default Configuration】 By default, the function of suppressing the sending of ARP requests to the authentication VLAN is enabled.

【Command Mode】 Interface mode

【Default Level】 2

【Usage Guide】 In the gateway authentication mode, all sub-VLANs under the SuperVLAN are authentication VLANs by default, and the authenticated users under the authentication VLAN need to be authenticated before they can access the Internet. After the user is authenticated, a static ARP entry will be generated on the device. Therefore, when the device accesses the authenticated user, it does not need to send an ARP request to the authentication VLAN. If the device needs to access users in the authentication-free VLAN, it only needs to send an ARP request to the authentication-free VLAN.

In the gateway authentication mode, the device enables the function of suppressing the sending of ARP requests to the authentication VLAN by default. If the device needs to access the authentication VLAN

For the authentication-free users under , this function needs to be turned off.

【Configuration Example]】1: Enable the function of suppressing the sending of ARP requests to the authentication VLAN on VLAN 2.

```
AC-FS(config)# interface vlan 2
AC-FS(config-if-VLAN 2)# arp suppress-auth-vlan-req
```

【Verification】1: The no arp suppress-auth-vlan-req command does not exist under the visible interface in show run interface vlan 2.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.12 arp timeout

Configure the timeout period for dynamic ARP entries in the ARP buffer.

arp timeout seconds

Restore Default Configuration.

no arp timeout

【Parameter Description】

Parameter	Description
seconds	The timeout, in seconds, in the range 0-2147483.

【Default Configuration】 The default timeout time is 3600 seconds.

【Command Mode】 Interface mode

【Default Level】 2

【Usage Guide】 ARP timeout setting only works on dynamically learned IP address and MAC address mapping. The shorter the timeout is set, the more realistic the mapping table is stored in the ARP buffer, but the more network bandwidth is consumed by ARP, so you need to weigh the pros and cons. Unless there are special needs, it is generally not necessary to configure the ARP timeout period.

【Configuration Example]】 1: Set the timeout period of the dynamic ARP mapping record learned from the Gigabit Ethernet port gigabitEthernet 0/1 to 120 seconds.

```
AC-FS(config)# interface gigabitEthernet 0/1
AC-FS(config-if-GigabitEthernet 0/1)# arp timeout 120
```

【Verification】 1: show arp timeout shows that the timeout time of interface 1 is 120 seconds.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

2.13 arp trusted

Configure the maximum number of trusted ARP entries.

arp trusted number

Restore Defaults.

no arp trusted

【Parameter Description】

Parameter	Description
number	Set the maximum number of trusted ARP entries, the minimum value is 10, and the maximum is the corresponding product arp capacity minus 1024.

【Default Configuration】 The maximum number of entries in the default trusted arp is half of the total capacity of the arp.

【Command Mode】 Global mode

【Default Level】 2

【Usage Guide】 To make this command take effect, first enable the trusted ARP function. Trusted ARP entries share memory with other entries. If too many trusted entries are occupied, there may be insufficient space for dynamic ARP entries. Generally set as needed, do not set too large.

【Configuration Example】1: The configuration can set up to 1000 trusted ARPs.

```
AC-FS(config)# arp trusted 1000
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.14 arp trust-monitor enable

Enable ARP trusted detection.

arp trust-monitor enable

Disable AR trusted detection.

no arp trust-monitor enable

【Parameter Description】-

【Default Configuration】 This function is closed.

【Command Mode】 Interface mode

【Default Level】 2

【Usage Guide】 This command is used to prevent arp spoofing from causing too many useless arp entries to occupy device resources. After enabling the arp trusted detection function on a Layer 3 interface, an arp request packet is received from the interface:

1. If the corresponding entry does not exist, create a dynamic arp entry, and enter NUD (neighbor unreachable detection) after a random time of 1 to 5 seconds, that is, set the newly learned arp entry to the aging state and unicast arp request, if the peer-end arp update is received within the aging time, the entry will be saved, otherwise the entry will be deleted directly.

2. If the corresponding arp entry already exists and the mac address has not been updated, the NUD detection logic will not be performed.

3. If the MAC address of the existing dynamic arp entry is updated, the NUD detection logic is also performed.

Since this function adds a strict confirmation process in the ARP learning process, enabling this function will affect the ARP learning performance. After this feature is turned off, the learning and updating of arp entries does not require a NUD process.

【Configuration Example】1: Enable ARP trusted detection function.

```
AC-FS(config)# interface gi 0/0
AC-FS(config-if-GigabitEthernet 0/0)# arp trust-monitor enable
```

2: Disable the ARP trusted detection function.

```
AC-FS(config)# interface gi 0/0
AC-FS(config-if-GigabitEthernet 0/0)# no arp trust-monitor enable
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.15 arp trusted aging

Configure trusted ARP to start aging.

arp trusted aging

Restore Defaults.

no arp trusted aging

【Parameter Description】 -

【Default Configuration】 GSN trusted ARP does not age by default.

【Command Mode】 Global mode

【Default Level】 2

【Usage Guide】 After using this command, the trusted ARP starts to age, and the aging time is the same as that of the dynamic ARP. The aging time can be set by the arp timeout command in interface mode.

【Configuration Example]】1: Configure trusted arp to start aging.

```
AC-FS(config)# arp trusted aging
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.16 arp trusted user-vlan

VLAN translation is performed when configuring trusted ARP entries.

arp trusted user-vlan vid1 translated-vlan vid2

Delete trusted ARP entries.

no arp trusted user-vlan vid1 translated-vlan vid2

【Parameter Description】

Parameter	Description
vid1	VID set by the server.
vid2	Converted VID.

【Default Configuration】 No VLAN conversion by default.

【Command Mode】 Global mode

【Default Level】 2

【Usage Guide】 To make this command take effect, first enable the trusted ARP function. This command needs to be configured only when the VLAN delivered by the server is different from the VLAN in which the trusted ARP takes effect.

【Configuration Example]】1: When the VLAN delivered by the server is 3, but the VLAN that the trusted ARP actually takes effect is 5, configure the following command:

```
AC-FS(config)# arp trusted user-vlan 3 translated-vlan 5
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.17 arp unresolve

Configure the maximum number of unresolved entries in ARP entries.

arp unresolve number

Restore Defaults.

no arp unresolve

【Parameter Description】

Parameter	Description
number	The maximum number of unresolved ARP entries, the minimum value is 1, and the maximum is the total capacity of ARP entries. The default value is the total capacity of ARP entries.

【Default Configuration】 The maximum number of unresolved entries that can be stored in the ARP buffer table is the total capacity of ARP entries.

【Command Mode】 Global mode

【Default Level】 2

【Usage Guide】 When a large number of unresolved entries are found in the ARP cache table, and they have not disappeared after a period of time, you can use this command to limit the number of unresolved entries.

【Configuration Examples】 The following example sets the maximum number of the unresolved items to 500.

```
AC-FS(config)# arp unresolve 500
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.18 clear arp-cache

Delete the dynamic ARP mapping record in the ARP buffer table. In the gateway authentication mode, the dynamic ARP entries under the authentication VLAN will not be deleted.

clear arp-cache [trusted] [ip [mask]] | interface interface-name]

【Parameter Description】

Parameter	Description
trusted	Deletes trusted ARP entries. Dynamic ARP entries are deleted by default.
ip	Deletes ARP entries of the specified IP address. If trustedvalue is specified, trusted ARP entries are deleted; otherwise, all dynamic ARP entries are deleted which is the default.
mask	Deletes ARP entries in a subnet mask. If trustedvalue is specified, trusted ARP entries in the subnet mask are deleted; otherwise, all dynamic ARP entries are deleted. The dynamic ARP entry specified by the IP address isdeleted by default.
interface-name	Deletes dynamic ARP entries on the specified interface. Dynamic ARP entries are deleted on all interfaces by default.

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】-

【Configuration Example]】1: Delete all ARP dynamic mapping record buffer tables:

```
AC-FS# clear arp-cache
```

2: Delete dynamic ARP entry 1.1.1.1:

```
AC-FS# clear arp-cache 1.1.1.1
```

3: Delete the dynamic ARP entry under interface SVI1:

```
AC-FS# clear arp-cache interface Vlan 1
```

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.19 ip proxy-arp

Enable the proxy ARP feature on the interface.

ip proxy-arp

Disable the proxy ARP function.

no ip proxy-arp

【Parameter Description】-

【Default Configuration】-

【Command Mode】 Interface mode

【Default Level】 2

【Usage Guide】 The proxy ARP function of the device can help the host without routing information to obtain the MAC address of the IP address of other networks or subnets. For example, when the device receives an ARP request, the IP address of the sender of the ARP request does not belong to the same network as the requested IP address, and the device knows the route of the requested IP address, the device will send an ARP response, and the MAC address of the response is the device. Own Ethernet MAC address. The above process is the function of proxy ARP.

【Configuration Example]】1: Enable proxy ARP function on gigabitEthernet 0/1:

```
AC-FS(config)# interface gigabitEthernet 0/1
AC-FS(config-if-GigabitEthernet 0/1)# ip proxy-arp
```

【Verification】1: When the proxy is turned on, show ip interface interface 1 shows that the Proxy ARP is: ON.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.20 local-proxy-arp

Enable the local proxy ARP feature on the SVI interface.

local-proxy-arp

Turn off the local proxy ARP function on the SVI interface.

no local-proxy-arp

【Parameter Description】-

【Default Configuration】-

【Command Mode】 Interface mode

【Default Level】 2

【Usage Guide】 After the device enables the local proxy ARP function, it can help the host to obtain the MAC addresses of other hosts in the subnet. For example, when port protection is enabled on the device, users on different ports are isolated at Layer 2. After the local ARP proxy function is enabled, the device receives an ARP request and sends an ARP response as a proxy. The MAC address of the response is the device's own. Ethernet MAC address, so that the communication between different hosts is realized by Layer 3 routing. This process is the function of local proxy ARP.

【Configuration Example]】1: Enable the local proxy ARP function on VLAN 1.

```
AC-FS(config)# interface vlan 1
AC-FS(config-if-VLAN 1)# local-proxy-arp
```

【Verification】1: When the local proxy ARP is turned on, show run interface <name> shows that the local-proxy-arp command exists under the interface.

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.21 service trustedarp

Enable the Trusted ARP feature.

service trustedarp

Disable the trusted ARP function.

no service trustedarp

【Parameter Description】-

【Default Configuration】 Disable trusted ARP by default

【Command Mode】 Global mode

【Default Level】 2

【Usage Guide】 The trusted ARP function of the device is a function of preventing ARP spoofing. As a part of the GSN scheme, it needs to be used together with the GSN scheme.

【Configuration Example]】1: In the global configuration mode, enable the service trustedarp function.

```
AC-FS(config)# service trustedarp
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】-

2.22 show arp

Displays the Address Resolution Protocol (ARP) buffer table.

show arp [interface-type interface-number | trusted [ip [mask]] | [ip [mask] | mac-address | static |

complete | incomplete]]

【Parameter Description】

Parameter	Description
interface-type interface-number	Displays the ARP of the specified Layer 3 port or Layer 2 port.
ip	IP address, displays the ARP entry of the specified IP address; if the trusted keyword is specified, only the trusted ARP entry is displayed, otherwise, the untrusted ARP entry is displayed.
mask	Displays ARP entries within the IP subnet; if the trusted keyword is specified, only trusted ones are displayed
static	ARP entry, otherwise display untrusted ARP entry.
complete	Shows all static arp entries, and shows the source of static arps.
incomplete	Displays all resolved dynamic arp entries.
mac-address	Displays all unresolved dynamic arp entries.

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】Display the ARP buffer table, in which the complete / incomplete keywords are used to display the resolved/unresolved entries in the dynamic ARP respectively.

【Configuration Example]】1: Display the output of show arp:

```
AC-FS# show arp
Total Numbers of Arp: 7
Protocol  Address          Age(min)  Hardware        Type    Interface
Internet  192.168.195.68   0.....0013.20a5.7a5f  arpa VLAN 1
Internet  192.168.195.67   0         001a.a0b5.378d   arpa     VLAN  1
Internet  192.168.195.65   0.....0018.8b7b.713e  arpa VLAN 1
Internet  192.168.195.64   0.....0018.8b7b.9106  arpa    VLAN 1
Internet  192.168.195.63   0         001a.a0b5.3990   arpa     VLAN  1
Internet  192.168.195.62   0         001a.a0b5.0b25  arpa  VLAN 1
```

Internet 192.168.195.5 -- 00d0.f822.33b1 arpa VLAN 1

2: Show output of show arp 192.168.195.68:

```
AC-FS# show arp 192.168.195.68
Protocol  Address    Age(min)  Hardware        Type Interface
Internet  192.168.195.68   1.....0013.20a5.7a5f  arpa  VLAN 1
```

3: Display the output of show arp 192.168.195.0 255.255.255.0:

```
AC-FS# show arp 192.168.195.0 255.255.255.0
Protocol  Address  Age(min)  Hardware  Type  Interface
Internet  192.168.195.64    0.....0018.8b7b.9106  arpa  VLAN 1
Internet 192.168.195.2   1   00d0.f8ff.f00e  arpa  VLAN 1
Internet  192.168.195.5---------00d0.f822.33b1  arpa  VLAN 1
Internet  192.168.195.1     0    00d0.f8a6.5af7  arpa    VLAN 1
Internet  192.168.195.51    1.....0018.8b82.8691  arpa    VLAN 1
```

4: Display the output of show arp 001a.a0b5.378d:

```
AC-FS# show arp 001a.a0b5.378d
Protocol  Address  Age(min)  Hardware  Type  Interface
Internet  192.168.195.67  4  001a.a0b5.378d  arpa  VLAN 1
```

5: Display the output of show arp static:

```
AC-FS# show arp static
Protocol  Address  Age(min)  Hardware  Type   Interface         Origin
Internet  192.168.23.55    <static>  0000.0000.0010  arpa   VLAN 100   Configure
Internet  192.168.23.56    <static>  0000.0000.0020  arpa   VLAN 100   Authentication
2  static arp entries exist.
```

Field Description:

Field	Description
Protocol	Currently there is only the value Internet, which represents the IP protocol.
Address	IPv4 address.
Age(min)	The current age of the entry, for the local IP, displays '-', for static entries, displays <static>, for dynamic entries, displays how long the entry has been learned, the unit is minutes.
Hardware	Hardware address, that is, 48-bit MAC address, each 16-bit group, separated by '.'. Hexadecimal representation.
Type	Currently only arpa is the value.
Interface	The Layer 3 interface corresponding to this ARP entry. For static ARP entries, sometimes there is no information in this place, because the IP of static ARP is not in any directly connected network segment of the device.
Origin	The source of static ARP entries. Configure is manually configured, and Authentication indicates that it is generated through authentication.

【Prompt Information】-

【Platform Description】-

2.23 show arp counter

Use this command to display the number of ARP entries in the ARP cache table. show arp counter

【Parameter Description】 -

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】-

【Configuration Examples】 1: Display the number of arp entries in the ARP cache table.

```
AC-FS# show arp counter
The Arp Entry counter:0
The Unresolve Arp Entry:0
```

【Prompt Information】-

【Platform Description】-

2.24 show arp packet statistics

Displays the statistics of ARP packets.

show arp packet statistics [interface-name]

【Parameter Description】

Parameter	Description
interface-name	Displays the statistics of ARP packets on the specified interface.

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】 -

【Configuration Examples】 1: Display ARP statistics table information:

```
AC-FS#show arp packet statistics
Interface              Received  Received Received  Sent      Sent
Name                   R
equests  Replies  Others    Requests  Replies
_____________________  ________  ________ ________  ________  _______

GigabitEthernet 0/0    0    0     0      0      0 GigabitEthernet 0/1
143649        232        0        2        0 GigabitEthernet 0/2     0
0      0 0 0    GigabitEthernet      0/3      0      0      0 0        0
GigabitEthernet  0/4      0          0          0          0          0
GigabitEthernet 0/5     0          0          0          0          0
GigabitEthernet 0/6  0  0  0  0  0 Loopback 1               0          0
0         0         0
```

Description of fields:

Field	Description
Received Requests	Number of received ARP requests.
Received Replies	Number of received ARP response message.
Received Others	Number of other received ARP packet.
Sent Requests	Number of sent ARP requests.
Sent Replies	Number of sent ARP requests.

【Related Commands】

Command	Description
N/A	N/A

【Prompt Information】 -

【Platform Description】 -

2.25 show arp timeout

Displays the aging time of dynamic ARP entries.

show arp timeout

【Parameter Description】 -

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】-

【Configuration Example】1: Display the aging time of dynamic ARP entries.

```
AC-FS# show arp timeout
Interface               arp timeout(sec)
----------------------  ----------------
VLAN 1                  3600
```

【Prompt Information】-

【Platform Description】-

2.26 show ip arp

Displays the Address Resolution Protocol (ARP) buffer table.

show ip arp

【Parameter Description】 -

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】-

【Configuration Examples】 1: Display the Address Resolution Protocol (ARP) buffer table.

```
AC-FS# show ip arp
Protocol Address        Age(min)Hardware  Type
Interface
Internet 192.168.7.233   23.....0007.e9d9.0488   ARPA FastEthernet 0/0
Internet 192.168.7.112   10.....0050.eb08.6617   ARPA FastEthernet 0/0
Internet  192.168.7.79   12   00d0.f808.3d5c   ARPA   FastEthernet   0/0
Internet   192.168.7.1   50   00d0.f84e.1c7f   ARPA   FastEthernet   0/0
Internet  192.168.7.215   36   00d0.f80d.1090   ARPA   FastEthernet   0/0
Internet 192.168.7.127   0      0060.97bd.ebee   ARPA FastEthernet 0/0
Internet 192.168.7.195   57.....0060.97bd.ef2d   ARPA FastEthernet 0/0
Internet 192.168.7.183------00d0.f8fb.108b   ARPA FastEthernet 0/0
```

Each field in the ARP cache table has the following meanings:

Field	Description
Protocol	Network address protocol, always Internet.
Address	The IP address corresponding to the hardware address.
Age (min)	Age of the ARP cache record, in minutes; If it is not locally or statically configured, the value of the field is represented with "-".
Hardware	Hardware address corresponding to the IP address
Type	The type of hardware address. The value is ARPA for all Ethernet addresses.
Interface	Interface associated with the IP address.

【Prompt Information】-

【Platform Description】-

3 DHCP

3.1 address range

To specify the range of address segments that can be assigned by a CLASS under the CLASS associated with a DHCP address pool, use the address range command in address pool class configuration mode.

address range low-ip-address high-ip-address

The no form of this command removes the segment range.

no address range

【Parameter Description】

Parameter	Description
low-ip-address	The starting address in the segment range.
high-ip-address	End address in the segment range.

【Default Configuration】 The default associated CLASS is not configured with a segment range, and the default is the segment range of the address pool.

【Command Mode】 Address pool CLASS configuration mode

【Usage Guide】 This command belongs to Server configuration; each CLASS corresponds to a segment range, and the segment range must be from low address to high address, and the segment range can be duplicated between multiple CLASSs. If the CLASS associated with the address pool is specified, but the corresponding segment range is not configured, the default segment range of the CLASS is the same as the segment range of the address pool in which the CLASS is located.

【Configuration Examples】 1: Configure the address pool mypool0 to associate class1 with the segment range 172.16.1.1-172.16.1.8.

```
AC-FS(config)# ip dhcp pool mypool0
AC-FS(dhcp-config)# class class1
AC-FS(config-dhcp-pool-class)# address range 172.16.1.1  172.16.1.8
```

【Verification】 The configuration is successful by show run

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

3.2 address-manage

Enter the configuration mode of the AM rule

address-manage

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 -

【Command Mode】 Global Configuration Mode

【Default Level】 14

【Usage Guide】 This command belongs to Server configuration and needs to be used with supervlan.

【Configuration Examples】 1: Enter the configuration mode of AM rule.

```
AC-FS(config)#address-manage
```

【Verification】 The configuration is successful by show run.

【Common Mistake】 -

【Platform Description】 -

3.3 bootfile

To define the default boot image file name for DHCP clients, use the DHCP address pool configuration command bootfile bootfile file-name.

The no form can be undefined

no bootfile

to restore the default value

default bootfile

【Parameter Description】

Parameter	Description
file-name	Define the name of the file used to start.

【Default Configuration】 No bootfile name is defined by default

【Command Mode】 DHCP address pool configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to Server configuration; some DHCP clients need to download operating system, configuration files, etc. during the boot process, the DHCP server must provide the image file name needed during the boot process, and only then the DHCP client can download the file through the corresponding server (e.g. TFTP). Other servers are defined by the next-server command

【Configuration Example]】 1: The device is enabled with DHCP server and relay features.

```
AC-FS(dhcp-config)# bootfile router.conf
```

【Verification】The configuration is successful by show run

【Prompt Information] -

【Common Mistake】 -

【Platform Description】 –

3.4 class

To configure the associated CLASS in a DHCP address pool, use the class command in DHCP address pool configuration mode.

class class-name

The no form can be undefined.

no class class-name

【Parameter Description】

Parameter	Description
class-name	Enter the name of the CLASS, either as a string or as a number, such as myclass or 1.

【Default Configuration】 The default address pool is not associated with any CLASS.

【Command Mode】 DHCP address pool configuration mode.

【Default Level】 14

【Usage Guide】 This command belongs to Server configuration; each DHCP address pool can assign addresses based on Option82 matching information. We match the Option82 information into categories, and specify the segment range that can be assigned for each of these categories in the DHCP address pool. This categorization is called CLASS, and a DHCP address pool can be associated with multiple CLASSs, each of which can specify a different segment range.

During the address allocation process, the address pools that can be allocated are first determined according to the client's network segment, then the CLASS to which the client belongs is further determined according to its Option82 information, and the IP address is allocated from the segment range corresponding to the CLASS. When a request message matches more than one CLASS in the address pool, the addresses are allocated from the corresponding CLASS segment range in the order of the CLASS configuration in the address pool, and if the CLASS has reached its allocated address limit, it will continue to be allocated from the next CLASS.

If the CLASS has reached its address limit, the next matching CLASS will be allocated, and so on. Each CLASS corresponds to a segment range and the segment range must be from the low address to the high address, allowing for duplication of segment ranges between multiple CLASSs. If the CLASS associated with the address pool is specified and no CLASS segment is configured, the default segment range of the CLASS is the same as the segment range of the address pool in which the CLASS is located.

【Configuration Example] 1: Configure the address pool mypool0 to associate with class1.

```
AC-FS(config)# ip dhcp pool mypool0
AC-FS(dhcp-config)# class class1
```

【Verification】The configuration is successful by show run

【Prompt Information】 -

【Common Mistake】 –

【Platform Description】 -

3.5 clear ip dhcp binding

To clear the DHCP binding table, use the clear ip dhcp binding command in privileged user mode.

clear ip dhcp binding { * | ip-address }

【Parameter Description】

Parameter	Description
*	Delete all DCHP bindings.
ip-address	Delete specified IP address records.

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】 This command belongs to Server configuration; this command can only clear DHCP automatic binding, DHCP manual binding can be deleted by no ip dhcp pool

command

【Configuration Example】1: Clear the DHCP binding with the IP address 192.168.12.100

```
AC-FS# clear ip dhcp binding 192.168.12.100
```

【Prompt Information】 -

【Platform Description】 -

3.6 clear ip dhcp conflict

To clear DHCP conflict records, use the clear ip dhcp conflict command in privileged user mode

clear ip dhcp conflict { * | ip-address }

【Parameter Description】

Parameter	Description
*	Delete all DCHP address conflict records.
ip-address	Delete specified IP address conflict records.

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】 The command belongs to Server configuration; DHCP server detects address conflict with ping session, DHCP client detects address conflict with Address Resolution Protocol (ARP). clear ip dhcp conflict can delete historical conflict records.

【Configuration Example]】1: All address conflict records are cleared.

```
AC-FS# clear ip dhcp conflict *
```

【Prompt Information】-

【Platform Description】 -

3.7 clear ip dhcp history

To clear the DHCP history, use the clear ip dhcp history command in privileged user mode.

clear ip dhcp history{ * | mac-address }

【Parameter Description】

Parameter	Description
*	Delete all DCHP address history.
mac-address	Delete the specified mac address history .

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】 This command belongs to the server clear; the server retains all the address information that has been assigned, clear ip dhcp history can delete the history record.

【Configuration Example]】 1: Clear all address history.

```
AC-FS# clear ip dhcp history *
```

【Prompt Information】-

【Platform Description】 -

3.8 clear ip dhcp server detect

To clear DHCP pseudo server records.

clear ip dhcp server detect { * | ip-address }

【Parameter Description】

Parameter	Description
*	Delete all DHCP pseudo server records.
ip-address	Deletes the specified DHCP pseudo server record.

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】 This command belongs to the server configuration; the server will keep the detected fake server address, clear ip dhcp server detect can clear the fake server record.

【Configuration Example】1: Clear all DHCP pseudo server records.

```
AC-FS# clear ip dhcp server detect *
```

【Prompt Information】-

【Platform Description】 -

3.9 clear ip dhcp server rate

Statistics on the processing rate of the packets to be reset by the DHCP server in each related module.

clear ip dhcp server rate

【Parameter Description】 -

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】 This command belongs to the server configuration; it is used to clear the dhcp server statistics on the processing rate of each packet in different modules, such as arp, hot backup, lsm, socket, etc.

【Configuration Example]】 1: Statistics on the processing rate of the packets to be reset by the DHCP server in each related module.

```
AC-FS# clear ip dhcp server rate
```

【Prompt Information】-

【Platform Description】 -

3.10 clear ip dhcp server statistics

To reset the counters of the DHCP server.

clear ip dhcp server statistics

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】This command belongs to Server configuration; DHCP server packet statistics, records the number of DHCP address pool, automatic binding, manual binding and expired binding, and makes statistics on various packets received and sent by the DHCP server. The clear ip dhcp server statistics command can delete the historical count records and start the statistics again.

【Configuration Example】1: Clear DHCP server statistics.

```
AC-FS# clear ip dhcp server statistics
```

【Prompt Information】-

【Platform Description】 -

3.11 clear ip dhcp relay statistics

Reset the counters for DHCP relay.

clear ip dhcp relay statistics

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】 This command belongs to Relay configuration; DHCP relay packet statistics, statistics on various types of packets received and sent by DHCP relay. The clear ip dhcp relay statistics command can delete the historical count records and start the statistics again.

【Configuration Example】1: Clear DHCP relay statistics.

```
AC-FS# clear ip dhcp relay statistics
```

【Prompt Information】-

【Platform Description】 -

3.12 client-identifier

To define a unique identifier for a DHCP client (in hexadecimal numbers separated by dots), use the DHCP address pool configuration.

command client-identifier client-identifier unique-identifier

The no form can delete the client ID.

no client-identifier

Restore Defaults.

default client-identifier

【Parameter Description】

Parameter	Description
unique-identifier	The identity of the DHCP client, in dot-separated hexadecimal. Such as: 0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31.

【Default Configuration】 No default value

【Command Mode】 DHCP address pool configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to the server configuration; some DHCP clients use the client ID instead of the hardware address to represent the client when requesting the DHCP server to assign an IP address. The client ID consists of the media type, MAC address and interface name. For example, if the MAC address is 00d0.f822.33b4 and the interface name is GigabitEthernet 0/1, the corresponding client ID is 0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31, where 01 represents the Ethernet media type,67.6967.6162.6974.4574.6865.726e.6574.302f.31 is the hexadecimal code of GigabitEthernet0/1. For the definition of media codes, please refer to the "Address Resolution Protocol Parameters" section of the RFC1700 document.
This command can be used only when DHCP manual binding is defined.

【Configuration Example]】 1: Defines the client ID of the Ethernet DHCP client whose MAC address is 00d0.f822.33b4.

```
AC-FS(dhcp-config)# client-identifier
0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31
```

【Verification】 It can be seen that the configuration is successful through show run.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.13 client-name

To define the name of the DHCP client, use the DHCP address pool configuration command client-name client-name client-name

no form deletes the name of the DHCP client.

no client-name

Restore Defaults.

default client-name

【Parameter Description】

Parameter	Description
client-name	Defines the name of the DHCP client. Any standard ASCII character set can be used. The name should not include the suffix domain name, such as defining river as the DHCP client name, cannot be defined as river.i-net.com.cn.

【Default Configuration】 The client name is not defined by default.

【Command Mode】 DHCP address pool configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to Server configuration; only when DHCP manual binding is defined, can this command be used to define the name of the DHCP client. The name should not include the suffix domain name.

【Configuration Example]】 1: A string river is defined as the name of the client.

```
AC-FS(dhcp-config)# lease 0 1
```

2: Set the DHCP lease to 1 minute.

```
AC-FS(dhcp-config)# lease 0 0 1
```

【Verification】 It can be seen that the configuration is successful through show run.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.14 default-router

To define the default gateway of the DHCP client, use the DHCP address pool configuration command default-router default-router ip-address [ip-address2…ip-address8]

The no form can delete the definition of the default gateway.

no default-router

Restore Defaults.

defaut default-router

【Parameter Description】

Parameter	Description
ip-address	Defines the IP address of the WINS server. Requires at least one.
ip-address2…ip-address8	(Optional) Up to 8 gateways can be configured. By default there is only one IP address.

【Default Configuration】 The default gateway is not defined by default.

【Command Mode】 DHCP address pool configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to the server configuration; generally, the DHCP client needs to obtain the default gateway information from the DHCP server. The DHCP server needs to assign at least one gateway IP address to the client, which must be on the same network segment as the address assigned to the client.

【Configuration Example]】1: 192.168.12.1 is defined as the default gateway.

```
AC-FS(dhcp-config)# default-router 192.168.12.1
```

【Verification】It can be seen that the configuration is successful through show run.

【Prompt Information】 1: Configure an illegal address.

【Common Mistake】 1. Configure a non-unicast address.

2. Configure more than 8 valid addresses.

【Platform Description】 -

3.15 dns-server

To define a DNS server for DHCP clients, use the DHCP address pool configuration command dns-server dns-server ip-address [ip-address2…ip-address8]

The no form removes the definition of the DNS server.

no dns-server

Restore Defaults.

defaut dns-server

【Parameter Description】

Parameter	Description
ip-address	Defines the IP address of the DNS server. Requires at least one.
ip-address2…ip-address8	(Optional) Up to 8 DNS servers can be configured.

【Default Configuration】 No DNS server is defined by default.

【Command Mode】 DHCP address pool configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to the server configuration; when defining multiple DNS servers, the priority written in the front is higher, and the DHCP client only has the same priority as the one in the front.

If the communication with the DNS server fails, the next DNS server will be selected.

When the FSOS software also acts as a DHCP client, it can transmit the DNS server information obtained through the client to the DHCP client.

【Configuration Example]】1: The DHCP client specifies the DNS server 192.168.12.3.

```
AC-FS(dhcp-config)# dns-server 192.168.12.3
```

【Verification】It can be seen that the configuration is successful through show run.

【Prompt Information】 1: Configure an illegal address.

【Common Mistake】 1. Configure a non-unicast address.

2. Configure more than 8 valid addresses.

3.16 domain-name

To define the suffix domain name of the DHCP client, use the DHCP address pool command domain-name domain-name domain-name

The no form can delete the suffix domain name.

no domain-name

Restore Defaults.

defaut domain-name

【Parameter Description】

Parameter	Description
domain-name	Define the suffix domain name string of the DHCP client.

【Default Configuration】 There is no suffix domain name by default.

【Command Mode】 DHCP address pool configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to the server configuration; after the DHCP client obtains the specified suffix domain name, when accessing the host with the same suffix domain name, it can directly pass the host name.

【Configuration Example]】1: Define the suffix domain name i-net.com.cn for the DHCP client.

```
AC-FS(dhcp-config)# domain-name i-net.com.cn
```

【Verification】It can be seen that the configuration is successful through show run.

【Prompt Information】 1: Configure an illegal address.

【Common Mistake】 1. Configure a non-unicast address.

2. Configure more than 8 valid addresses.

3.17 dynamic-pool

To notify the thin AP to dynamically calculate the network number and netmask of the DHCP address pool based on the device MAC, you can configure the dynamic-pool command in the ap-config/or ap-group mode of the AC.

dynamic-pool

Deleting definitions in AC's ap-config/or ap-group mode.

no dynamic-pool

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 Default is not defined.

【Command Mode】 ap-config/ap-group

【Default Level】 14

【Usage Guide】 This command belongs to the AC server configuration.

【Configuration Example]】 1: Deliver thin APs to calculate dynamic pools based on MAC addresses.

AC-FS(config-group) # dynamic-pool

【Verification】 It can be seen that the configuration is successful through show run.

【Prompt Information】-

【Common Mistake】-

3.18 force-no-router

Forcing no gateway to be assigned to clients, configured in DHCP address pool mode.

force-no-router

The no form can be deleted to force the gateway not to be assigned.

no force-no-router

Restore Defaults.

default force-no-router

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 The default gateway is assigned to the client.

【Command Mode】 DHCP address pool configuration mode.

【Default Level】 14

【Usage Guide】 This command belongs to Server configuration; it is used to configure no gateway to clients when assigning addresses.

【Configuration Example]】 1: Do not assign a gateway to the client.

```
AC-FS(dhcp-config)# force-no-router
```

【Verification】 It can be seen that the configuration is successful through show run.

【Prompt Information】-

【Common Mistake】-

3.19 hardware-address

To define the hardware address of a DHCP client, use the DHCP address pool configuration command hardware-address

hardware-address hardware-address[type]

The no form can delete the definition of the hardware address.

no hardware-address

Restore Defaults.

defaut hardware-address

【Parameter Description】

Parameter	Description
hardware-address	Define the MAC address of the DHCP client
type	Identifies the hardware platform protocol of the DHCP client, which can be defined as a string or a number. String options: ethernet ieee802 Numeric options: 1 (10M ethernet) 6 (IEEE 802)

【Default Configuration】 No hardware address by default.

If no option is added when defining the hardware address, the default is ethernet.

【Command Mode】 DHCP address pool configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to Server configuration; this command can be used only when DHCP manual binding is defined.

【Configuration Example】1: Define the MAC address of type ethernet 00d0.f838.bf3d

```
AC-FS(dhcp-config)# hardware-address 00d0.f838.bf3d
```

【Verification】It can be seen that the configuration is successful through show run

【Prompt Information】 -

【Common Mistake】 -

3.20 0host

To define the IP address and netmask of the DHCP client host, use the DHCP address pool configuration command host host ip-address [netmask]

The no form removes the definition of the DHCP client IP address and netmask.

no host

Restore Defaults.

defaut host

【Parameter Description】

Parameter	Description
host ip-address [netmask]	Define the IP address of the DHCP client host.
netmask	Defines the netmask of the DHCP client host.

【Default Configuration】 The IP address and netmask of the host are not defined.

【Command Mode】 DHCP address pool configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to Server configuration; if the netmask is not clearly defined, the DHCP server will use the natural netmask of the IP address. Class A addresses have a netmask of 255.0.0.0; class B addresses have a netmask of 255.255.0; and class C addresses have a netmask of 255.255.255.0.

This command can be used only when DHCP manual binding is defined.

【Configuration Example]】1: Set the client IP address to 192.168.12.91 and the mask to avoid 255.255.255.240

```
AC-FS(dhcp-config)# host 192.168.12.91 255.255.255.240
```

【Verification】 It can be seen that the configuration is successful through show run.

【Prompt Information】 1: Configure an illegal address.

```
AC-FS(dhcp-config)# host 225.2.2.2 255.0.0.0
% Error: ip address 225.2.2.2 is not valid!
```

【Common Mistake】 1. Configure an illegal address.

3.21 ip address dhcp

To enable Ethernet or PPP, HDLC, FR encapsulated interfaces to obtain IP address information through DHCP, use the interface configuration command ip address dhcp.

ip address dhcp

no form can cancel the configuration.

no ip address dhcp

Restore Defaults.

defaut ip address dhcp

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 The default interface cannot obtain an IP address through DHCP.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to the Client configuration; the DHCP client of the RGOS software also requires the DHCP server to provide five configuration parameters when requesting an IP address: 1) DHCP option 1, client subnet mask; 2) DHCP option 3. Gateway information on the same subnet; 3) DHCP option 6, DNS server information; 4) DHCP option 15, host suffix domain name; DHCP option 44, WINS server information (optional configuration). The client of RGOS software allows to obtain addresses through dhcp on PPP, FR and HDLC connections. This requires the support of the server. At present we of servers support this feature.

【Configuration Example]】 1: Make FastEthernet 0 port automatically obtain an IP address.

```
AC-FS(config)# interface GigabitEthernet 0/1
AC-FS(config-if-GigabitEthernet 0/1) ip address dhcp
```

【Verification】 It can be seen that the configuration is successful through show run.

【Prompt Information】 -

【Common Mistake】 1. Open an account on the Layer 2 interface.

3.22 ip dhcp class

To define a CLASS and enter global CLASS configuration mode, use the ip dhcp class command in global configuration mode.

ip dhcp class class-name

The no form can delete the global CLASS.

no ip dhcp class class-name

【Parameter Description】

Parameter	Description
class-name	Enter the name of the CLASS, which can be a string or a number, such as myclass or 1.

【Default Configuration】 No class is configured by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to Server configuration; executing this command will enter the global CLASS configuration mode. In this configuration mode, you can configure Option82 information matched by CLASS, identification information of CLASS.

【Configuration Example]】 1: Configure a global CLASS.

```
AC-FS(config)# ip dhcp class myclass
```

【Verification】It can be seen that the configuration is successful through show run.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.23 ip dhcp client class-id

Customize the content of the class-id field in the request packet sent by the HDCP client.

ip dhcp client class-id { ascii | hex } string

no form can restore the default configuration.

no ip dhcp client class-id

Restore Defaults.

default ip dhcp client class-id

【Parameter Description】

Parameter	Description
hex	The format of the padding content is a hexadecimal number.
ascii	The format of the filling content is ascii code.
string	class-id custom content.

【Default Configuration】 Default Configuration is the manufacturer's identification information.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to Client configuration; customize the content of class-id in the request message

【Configuration Example】 Configure the class-id as AC-FS-EG1000C on interface GigabitEthernet 0/1

```
AC-FS(config-if-GigabitEthernet 0/1)#ip dhcp client class-id ascii AC-FS-EG1000C
```

【Verification】 It can be seen that the configuration is successful through show run.

【Prompt Information】-

【Common Mistake】-

3.24 ip dhcp client client-id

Customize the content of the client-id field in the request packet sent by the HDCP client.

ip dhcp client client-id { ascii string | hex string | exclude interface-name }

no form can restore the configuration.

no ip dhcp client client-id

Restore Defaults.

default ip dhcp client client-id

【Parameter Description】

Parameter	Description
hex	The format of the padding content is a hexadecimal number.
ascii	The format of the filling content is ascii code.
string	client-id custom content.
exclude interface-name	client-id field does not contain interface name.

【Default Configuration】 Default Configuration is interface type + MAC address + interface name.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to Client configuration; customize the content of client-id in the request message.

【Configuration Example]】 Configure the client-id as 0102.0304.0506 on interface GigabitEthernet 0/1.

```
AC-FS(config-if-GigabitEthernet 0/1)#ip dhcp client client-id hex 0102.0304.0506
```

【Verification】 It can be seen that the configuration is successful through show run.

【Prompt Information】-

【Common Mistake】-

3.25 ip dhcp client hostname

Customize the content of the hostname field in the request packet sent by the HDCP client.

ip dhcp client hostname string

no form can restore the configuration.

no ip dhcp client hostname

Restore Defaults.

default ip dhcp client hostname

【Parameter Description】

Parameter	Description
string	hostname custom content.

【Default Configuration】 Default Configuration is the host name.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to Client configuration; customize the content of hostname in the request message.

【Configuration Example】 Configure hostname as AC-FS under interface GigabitEthernet 0/1.

```
AC-FS(config-if-GigabitEthernet 0/1)#ip dhcp client hostname AC-FS
```

【Verification】 It can be seen that the configuration is successful through show run.

【Prompt Information】-

【Common Mistake】-

3.26 ip dhcp client lease

Customize the content of the lease field in the request message sent by the HDCP client.

ip dhcp client lease days [hours] [minutes]

no form can restore the configuration.

no ip dhcp client lease

Restore Defaults.

default ip dhcp client lease

【Parameter Description】

Parameter	Description
days	Time to define the lease period, in days.
hours	(Optional) The time in hours that defines the lease term. Days must be defined before hours can be defined. Lack Province is 0.
minutes	(Optional) The time in minutes that defines the lease period. Days and hours must be defined before minutes are defined number, default is 0.

【Default Configuration】 In Default Configuration, the request message does not contain the lease field.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to Client configuration; customize the content of lease in the request message.

【Configuration Example】 Configure lease as 1 hour on interface GigabitEthernet 0/1.

```
AC-FS(config-if-GigabitEthernet 0/1)#ip dhcp client lease 0 1
```

【Verification】 It can be seen that the configuration is successful through show run.

【Prompt Information】 -

【Common Mistake】 -

3.27 ip dhcp client option-list include

Customize the content of the option-list field in the request message sent by the HDCP client.

ip dhcp client option-list include string

no form can restore the configuration.

no ip dhcp client option-list include

Restore Defaults.

default ip dhcp client option-list include

【Parameter Description】

Parameter	Description
string	Define which fields need to be included in the option-list field.

【Default Configuration】 In Default Configuration, option-list only contains necessary fields.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to the client configuration; customize the content of the option-list in the request message.

【Configuration Example】The option-list configured on interface GigabitEthernet 0/1 contains 66,67,43.

```
AC-FS(config-if-GigabitEthernet 0/1)#ip dhcp client option-list include 66-67,43
```

【Verification】It can be seen that the configuration is successful through show run.

【Prompt Information】-

【Common Mistake】-

3.28 ip dhcp excluded-address

To define certain IP addresses so that the DHCP server will not assign them to DHCP clients, use the global configuration command.

ip dhcp excluded-address low-ip-address [high-ip-address]

The no form of the command cancels this definition.

no ip dhcp excluded-address low-ip-address [high-ip-address]

Restore Default Configuration.

default ip dhcp excluded-address low-ip-address [high-ip-address]

【Parameter Description】

Parameter	Description
low-ip-address	Exclude IP addresses, or exclude IP addresses at the beginning of a range of IP addresses.
high-ip-address	The ending IP address of the exclusive address range. By default its value is low-ip-address.

【Default Configuration】 The default DHCP server assigns the IP addresses of the entire address pool.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to Server configuration; if no exclusive IP address is configured, the DHCP server will try to assign all IP addresses in the DHCP address pool. This command can reserve some IP addresses for specific hosts and avoid these addresses being assigned to DHCP clients. Precisely define exclusive IP addresses and also reduce conflict detection time when DHCP server assigns addresses.

【Configuration Example】1: The DHCP server will not try to assign IP addresses in the range of 192.168.12.100~150.

```
AC-FS(config)#ip dhcp excluded-address 192.168.12.100 192.168.12.150
```

2: Delete the excluded address range in Example 1

```
AC-FS(config)#no ip dhcp excluded-address 192.168.12.100 192.168.12.150
```

【Verification】 You can observe the successful configuration through show run.

【Prompt Information】 1: Configure illegal exclusion addresses.

```
AC-FS(config)#ip dh excluded-address 225.1.1.1
% Error:  Ip address 225.1.1.1 or 225.1.1.1 is not valid!
```

2: Delete non-existing excluded addresses.

```
AC-FS(config)#no ip dhcp excluded-address 20.1.1.1
% Range [20.1.1.1, 20.1.1.1] is not in the database.
```

【Common Mistake】 1. Configure illegal exclusion addresses.

2. Delete non-existing excluded addresses.

【Platform Description】 -

3.29 ip dhcp force-send-nak

To configure the function of forcibly sending NAK packets.

ip dhcp force-send-nak

Cancel the function of forcibly sending NAK messages.

no ip dhcp force-send-nak

Restore Default Configuration.

default ip dhcp force-send-nak

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 Enable the function of forcibly sending NAK packets under Default Configuration.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to the server configuration; the DHCP client will check the previously used IP address every time the device starts, and send a DHCPREQUEST request message to renew the contract, hoping to use the IP address again. If the address is unavailable, the DHCP server sends a NAK message to make the client re-initiate DHCPDISCOVER to apply for a new address. If the current server does not have a corresponding lease record, the client will continue to send a DHCPREQUEST lease renewal request. In wireless applications, in order to speed up the user's re-initiation of a DHCPDISCOVER request, the function of forcing a NAK message to be sent is added.

【Configuration Example]】1: Enable the forced NAK function in global configuration mode.

```
AC-FS(config)# ip dhcp force-send-nak
```

【Verification】 You can see that the configuration is successful through show run.

【Common Mistake】-

【Platform Description】 -

3.30 ip dhcp monitor-vrrp-state

To monitor the status of VRRP, the DHCP Server only processes the request packets from the vrrp interface that is currently in the Master state.

ip dhcp monitor-vrrp-state

Cancel the monitoring of the vrrp status. At this time, the request packets from the VRRP interface in the Master or Backup status will be processed.

no ip dhcp monitor-vrrp-state

Restore Default Configuration.

default ip dhcp monitor-vrrp-state

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Layer 3 interface configuration mode

【Default Level】 14

【Default Configuration】 In Default Configuration, the interface VRRP status is not monitored.

【Usage Guide】 This command belongs to server configuration; if VRRP addresses are configured on an interface, the DHCP server only processes the request packets of the interface in the master state and discards the request packets of the interface in the non-master

state. For interfaces without VRRP addresses configured, the DHCP server will no longer monitor the VRRP status, and all DHCP request packets will be processed.

【Configuration Example]】 1: The DHCP server monitors the VRRP status of the current Layer 3 interface.

```
AC-FS(config-if)# ip dhcp monitor-vrrp-state
```

【Verification】 -

【Prompt Information】 1: Configure VRRP status monitoring on the Layer 2 interface.

```
AC-FS(config-if-GigabitEthernet 0/2)#ip dhcp monitor-vrrp-state
% Invalid input detected at '^' marker.
```

【Common Mistake】 1: Configure VRRP status monitoring on the Layer 2 interface.

【Platform Description】 -

3.31 ip dhcp ping packets

To configure the number of times the DHCP server pings the address when it detects an address conflict.

ip dhcp ping packets [number]

no form restores Default Configuration.

no ip dhcp ping packets

Restore Default Configuration.

default ip dhcp ping packets

【Parameter Description】

Parameter	Description
number	(Optional) Range from 0 to 10, where 0 turns off ping. By default ping two packets.

【Default Configuration】 The default number of ping packets is 2.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to Server configuration; when the DHCP server tries to assign an IP address from the DHCP address pool, it will use the ping operation to detect whether the address has been occupied by other hosts. DHCP client. Ping operation defaults to send two packets, up to 10 packets can be sent.

【Configuration Example]】 1: Set the number of packets sent by the ping operation to 3.

```
AC-FS(config)# ip dhcp ping packets 3
```

【Verification】You can see that the configuration is successful through show run.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

3.32 ip dhcp ping timeout

To configure the timeout period for the DHCP server to wait for a response when pinging to detect an address conflict.

ip dhcp ping timeout milli-seconds

no form can restore Default Configuration.

no ip dhcp ping timeout

Restore Default Configuration.

default ip dhcp ping timeout

【Parameter Description】

Parameter	Description
milli-seconds	The time in milliseconds that the DHCP server waits for a ping reply. Value range is 100 to 10000.

【Default Configuration】 The default timeout is 500 milliseconds.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to Server configuration; defines the time to wait for a ping reply packet.

【Configuration Example】 1: Set the ping response packet waiting time to 600ms.

```
AC-FS(config)# ip dhcp ping timeout 600
```

【Verification】 You can see that the configuration is successful through show run.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

3.33 ip dhcp pool

To define a DHCP address pool name and enter DHCP address pool configuration mode.

ip dhcp pool pool-name

no form can delete the DHCP address pool.

no ip dhcp pool pool-name

Restoring Defaults Deleting an Address Pool.

default ip dhcp pool pool-name

【Parameter Description】

Parameter	Description
pool-name	address pool name.

【Default Configuration】 No DHCP address pool is defined by default.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】 This command belongs to Server configuration;

1: Execute this command, it will enter the DHCP address pool configuration mode, which is displayed as:

```
AC-FS(dhcp-config)#
```

In this configuration mode, you can configure parameters such as IP address range, DNS server, default gateway, etc.

【Configuration Example]】 1: A DHCP address pool named mypool0 is defined.

```
AC-FS(config)#ip dhcp pool mypool0
AC-FS(dhcp-config)#
```

【Verification】 The configuration can be observed successfully through show ip dhcp pool mypool0.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.34 ip dhcp refresh arp

Re-deliver trusted ARP

ip dhcp refresh arp

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 -

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to Server configuration;

Executing this command will re-issue the trusted ARP according to the lease allocated from the address pool where update arp is configured.

【Configuration Example]】 1: Re-deliver trusted ARP.

```
AC-FS(config)#ip dhcp refresh arp
```

【Verification】 You can see the re-issued trusted ARP through show arp trusted.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

3.35 ip dhcp relay check server-id

Enable DHCP relay check server-di function.

ip dhcp relay check server-id

Disable the DHCP relay check server-id function.

no ip dhcp relay check server-id

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 Disable the DHCP relay check server-id function.

【Command Mode】 Global mode

【Default Level】 -

【Usage Guide】 This command belongs to Server configuration; when the command ip dhcp relay check server-id is configured, DHCP Relay only forwards DHCP request packets to the server specified in option server-id. If this command is not configured, the DHCP request message will be forwarded to all configured DHCP servers.

【Configuration Example】 1: Enable DHCP relay check server-di function.

```
AC-FS(config)# ip dhcp relay check server-id
```

2: Disable the DHCP relay check server-id function.

```
AC-FS(config)# no ip dhcp relay check server-id
```

【Verification】 1: Use the show running-config command to check whether the configuration is successful.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.36 ip dhcp relay information option82

Enable DHCP option82 function.

ip dhcp relay information option82

Disable the DHCP option82 function.

no ip dhcp relay information option82

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 Disable the DHCP option82 function.

【Command Mode】 Global mode

【Default Level】-

【Usage Guide】 This command belongs to relay configuration; when the command ip dhcp relay information option82 is configured, the device acts as a DHCP relay, and adds option information to the DHCP request message during the process of forwarding the DHCP request message.

【Configuration Example】 1: Enable DHCP option82 function.

```
AC-FS(config)# ip dhcp relay information option82
```

2: Disable the DHCP option82 function.

```
AC-FS(config)# no ip dhcp relay information option82
```

【Verification】 1: Use the show running-config command to check whether the configuration is successful.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.37 ip dhcp relay suppression

Enable DHCP relay suppression.

ip dhcp relay suppression

Disable the DHCP relay suppresson function.

no ip dhcp relay suppression

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 Disable the DHCP relay suppression function.

【Command Mode】 Interface mode

【Default Level】-

【Usage Guide】 This command belongs to relay configuration; after the command ip dhcp relay suppression is configured on the specified interface, the received messages on the interface will be blocked.

DHCP request packets; DHCP request packets received on other interfaces are forwarded normally.

【Configuration Example]】 1: Enable the DHCP relay suppresson function.

```
AC-FS(config-if)# ip dhcp relay suppression
```

2: Disable the DHCP relay suppresson function.

```
AC-FS(config-if)# no ip dhcp relay suppression
```

【Verification】 1: Use the show running-config command to check whether the configuration is successful.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

3.38 ip dhcp relay source

Specifies the source address of the relay packet.

ip dhcp relay source ip-address

Disables the source address of the specified relay packet.

no ip dhcp relay source

【Parameter Description】

Parameter	Description
ip-address	Source address of relay packets.

【Default Configuration】 The source address of the relay packet is not specified.

【Command Mode】 Interface mode

【Default Level】 14

【Usage Guide】 This command belongs to relay configuration; in some networking, the interface IP addresses of multiple DHCP relays are the same, the user needs to configure this command to specify the IP address of another interface on the relay device to fill in the relay packet. source address and Giaddr fields. Only one source address of a relay packet can be specified on an interface.

【Configuration Example】 1: Specify the source address of the relay packet.

```
AC-FS(config-if)# ip dhcp relay source 1.1.1.1
```

2: Disable the function of specifying the source address of the DHCP relay.

```
AC-FS(config-if)# no ip dhcp relay source
```

【Verification】 1: Use the show running-config command to check whether the configuration is successful.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

3.39 ip dhcp server detect

Enable DHCP fake server detection.

ip dhcp server detect

Disable DHCP fake server detection.

no ip dhcp server detect

Restore the default disable DHCP fake server detection function.

default ip dhcp server detect

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 Disable the DHCP pseudo server function.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 This command belongs to the server configuration; after configuring the DHCP fake server detection function, if there is a fake server in the network, it will be recorded in the log.

【Configuration Example】 1: Enable DHCP pseudo server function.

```
AC-FS(config)# ip dhcp server detect
```

【Verification】1: Use the show running-config command to check whether the configuration is successful.

【Prompt Information】-

【Common Mistake】

【Platform Description】 -

3.40 ip dhcp use class

To configure and enable CLASS for address assignment, use the ip dhcp use class command in global configuration mode. The no form of this command disables the use of CLASS for address assignment.

ip dhcp use class

no ip dhcp use class

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 By default, CLASS is enabled for address allocation.

【Command Mode】 Global configuration mode.

【Usage Guide】 This command belongs to Server configuration;

【Configuration Example]】 1: Configure to enable CLASS for address allocation.

```
AC-FS(config)# ip dhcp use class
```

【Verification】 You can see that the configuration is successful through show run.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.41 ip helper-address

Add a global DHCP server address.

ip helper-address { cycle-mode | A.B.C.D }

Delete a global DHCP server address.

no ip helper-address { cycle-mode | A.B.C.D }

【Parameter Description】

Parameter	Description
cycle-mode	Enable dhcp request packet forwarding to all dhcp servers.
A.B.C.D	DHCP server address.

【Default Configuration】 The DHCP server list is empty.

【Command Mode】 Global mode

【Default Level】-

【Usage Guide】 This command belongs to Relay configuration; after configuring the IP address of the DHCP server, the device will forward the received DHCP request message to it; at the same time, it will forward the received DHCP server response message to the DHCP client.

DHCP Server Address Global Configuration Up to 20 DHCP server addresses can be configured.

In the global configuration mode, the cycle-mode Parameter of the dhcp relay can be configured. When cycle-mode is enabled, it means that the dhcp relay is allowed to forward the received dhcp client request packets to all dhcp servers in the above rules; when cycle-mode is not enabled -mode means that dhcp relay only forwards the received dhcp client request message to the first dhcp server in the above rule. cycle-mode is enabled by default under global configuration.

【Configuration Example】1: Configure a global DHCP server IP address 192.168.100.1.

```
AC-FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z. AC-
FS(config)# ip helper-address 192.168.100.1
```

2: Delete the previously configured global DHCP server IP address 192.168.100.1.

```
AC-FS(config)# no ip helper-address 192.168.100.1
```

3: Enable dhcp request packet forwarding to all dhcp servers.

```
AC-FS(config)# ip helper-address cycle-mode
```

4: Disable the forwarding of dhcp request packets to all dhcp servers.

```
AC-FS(config)# no ip helper-address cycle-mode
```

【Verification】 1: Use the show running-config command to check whether the configuration is successful.

【Prompt Information】 -

【Common Mistake】 1: The ip helper-address configuration command can only be configured in global mode.

2: Before enabling the ip helper-address function, make sure that the DHCP Relay function has been enabled.

【Platform Description】 -

3.42 lease

To define the lease time that the DHCP server assigns addresses to clients, use the DHCP address pool configuration command lease. The no form of this command restores the Default Configuration. Limited leases ranging from 1 minute to 365 days 23 hours 59 minutes.

lease {days [hours] [minutes] | infinite}

no form restores Default Configuration.

no lease

Restore Defaults.

defaut lease

【Parameter Description】

Parameter	Description
days	Time to define the lease period, in days.

hours	(Optional) The time in hours that defines the lease term. Days must be defined before hours can be defined. Lack Province is 0.
minutes	(Optional) The time in minutes that defines the lease period. Days and hours must be defined before minutes are defined number, default is 0.
infinite	Define an unlimited lease term.

【Default Configuration】 The default lease period of the static address pool is infinite. The default lease period for other address pools is one day.

【Command Mode】 DHCP address pool configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to the server configuration; when the lease expires, the DHCP client will send a lease renewal request. The DHCP server generally allows renewal of the lease, and the renewed address remains unchanged.

【Configuration Example】 1: Set the DHCP lease to 1 hour.

```
AC-FS(dhcp-config)# lease 0 1
```

2: Set the DHCP lease to 1 minute

```
AC-FS(dhcp-config)# lease 0 0 1
```

【Verification】 It can be seen that the configuration is successful through show run.

【Prompt Information】-

【Common Mistake】-

3.43 lease-threshold

To define the alarm percentage for a DHCP address pool, use the DHCP address pool configuration command lease-threshold lease-threshold percentage

no form closes the alarm function.

no lease-threshold

Restore Defaults.

defaut lease-threshold

【Parameter Description】

Parameter	Description
percentage	Defines the percentage of address pool alarms, ranging from 60 to 100.

【Default Configuration】 The default is 90%

【Command Mode】 DHCP address pool configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to Server configuration; if the maximum IP utilization of the address pool reaches the threshold, the DHCP server will generate SYSLOG alarm information. IP utilization represents the ratio of the number of currently allocated addresses to the total number of addresses that can be allocated in the current address pool. If the number of allocated addresses is always above the alarm threshold, an alarm message will be generated every 5 minutes

【Configuration Example]】 1: Set the address pool alarm threshold to 80%:

```
AC-FS(dhcp-config)# lease-threshold 80
```

2: Disable the address pool alarm function.

```
AC-FS(dhcp-config)# no lease-threshold
```

【Verification】 It can be seen that the configuration is successful through show run.

【Prompt Information】-

【Common Mistake】-

3.44 manage-address-pool

To define the type of DHCP address pool as management address pool, use the DHCP address pool configuration command manage-address-pool.

manage-address-pool

The no form closes the management address pool attribute.

no manage-address-pool

Restore Defaults.

default manage-address-pool

【Default Configuration】 The address pool type is not configured.

【Command Mode】 DHCP address pool configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to the server configuration; it is only used to display the type of the address pool; the address pool type setting can be directly overwritten (that is, you can directly configure the user-addrss-pool, and change the address pool from the management address pool to the user address pool) ;When canceling the address pool type configuration, the type needs to match (that is, executing no/default manage-address-pool will set the management address pool to an unconfigured state).

【Configuration Example]】1: Set the address pool as the management address pool:

```
AC-FS(dhcp-config)# manage-address-pool
```

2: Turn off the address pool attribute

```
AC-FS(dhcp-config)# no manage-address-pool
```

【Verification】 It can be seen that the configuration is successful through show run.

【Prompt Information】-

【Common Mistake】-

3.45 match ip

To define matching rules for AM rules, use the command match ip:

match ip ip-address netmask [interface] [add/remove] vlan vlan-list

The no form can delete the definition;

no match ip ip-address netmask [interface] [add/remove] vlan vlan-list

【Parameter Description】

Parameter	Description
ip-address	website address.
netmask	address mask.
interface	interface name.
add/remove	Add or remove specified vlan.
vlan-list	vlan index.

【Default Configuration】 No default behavior.

【Command Mode】 AM rule configuration mode

【Default Level】 14

【Usage Guide】 1: After configuring this command, the DHCP client from the specified vlan + port will obtain the address in the configuration room.

2: In the supervlan scenario, users who satisfy the Dhcp static address pool configuration will only be assigned the static address no matter which subvlan they are in. At this time, the AM does not need to configure the address based on all subvlan/port, but only needs to configure the address in the corresponding subvlan. The vlan interval can take effect. Currently, this rule only takes effect for static address allocation, and does not take effect for dynamic addresses.

【Configuration Example]】 1: A matching rule is defined - the source is vlan index 10, and the configuration rule for a DHCP client with interface name GigabitEthernet 0/10 is: network number 192.168.11.0, mask 255.255.255.0.

```
AC-FS(config-address-manage)#match ip 192.168.11.0 255.255.255.0 GigabitEthernet 0/10 vlan 10
```

【Verification】 It can be seen that the configuration is successful through show run.

【Prompt Information】-

【Common Mistake】-

3.46 match ip default

To define a default match rule for AM rules, use the command match ip default;

match ip default ip-address netmask

The no form can delete the definition;

no match ip default ip-address netmask

【Parameter Description】

Parameter	Description
ip-address	website address.
netmask	address mask.

【Default Configuration】 No default behavior

【Command Mode】 AM rule configuration mode

【Default Level】 14

【Usage Guide】 After this command is configured, all DHCP clients from unconfigured vlan + port/vlan will obtain the address within the default range. If there is no such configuration command and no other vlan + port configuration, the allocation will be done according to the normal process.

【Configuration Example]】 1: The default matching rule is defined: the network number is 192.168.12.0, and the mask is 255.255.255.0

```
AC-FS(config-address-manage)#match ip default 192.168.12.0 255.255.255.0
```

【Verification】 It can be seen that the configuration is successful through show run.

【Prompt Information】-

【Common Mistake】-

3.47 netbios-name-server

To configure the WINS name server for Microsoft DHCP client NETBIOS.

netbios-name-server ip-address [ip-address2…ip-address8]

Delete the WINS server.

no netbios-name-server

Restore Defaults.

defaut netbios-name-server

【Parameter Description】

Parameter	Description
ip-address	Defines the IP address of the WINS server. Requires at least one.
ip-address2…ip-address8	(Optional) Up to 8 WINS servers can be configured.

【Default Configuration】 No WINS server is defined by default.

【Command Mode】 DHCP address pool configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to the server configuration; when defining multiple WINS servers, the priority written in the front is higher, and the DHCP client only has the same priority as the one in the front.

WINS server communication fails, the next WINS server will be selected.

【Configuration Example]】 1: The WINS server 192.168.12.3 is specified for the DHCP client.

```
AC-FS(dhcp-config)# netbios-name-server 192.168.12.3
```

【Verification】 It can be seen that the configuration is successful through show run.

【Prompt Information】 1: Configure an illegal address.

```
AC-FS(dhcp-config)#netbios-name-server 225.2.2.2
%Error: ip address (225.2.2.2) is not valid!
```

【Common Mistake】 1. Configure a non-unicast address.

2. Configure more than 8 valid addresses.

3.48 netbios-node-type

To define the primary NetBIOS node type for Microsoft DHCP clients, use the DHCP address pool configuration command

netbios-node-type netbios-node-type type

Remove NetBIOS node type configuration.

no netbios-node-type

Restore Defaults.

defaut netbios-node-type

【Parameter Description】

Parameter	Description
type	There are two ways to define the NetBIOS node type. Number definition, the range is from 0~FF, hexadecimal number, but can only take the following values: stands for b-node stands for p-node stands for m-node 8, representing h-node String definition: b-node, broadcast node p-node, peer-to-peer node m-node, hybrid node h-node, compound node

【Default Configuration】 No NetBIOS node type is defined by default.

【Command Mode】 DHCP address pool configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to Server configuration; Microsoft DHCP client has four types of NetBIOS nodes: 1) Broadcast, broadcast node, NetBIOS name resolution through broadcast; 2) Peer-to-peer, peer node, Perform NetBIOS name resolution by directly requesting the WINS server; 3) Mixed, a hybrid node, first request name resolution by broadcasting, and then perform name resolution by connecting with the WINS server; 4) Hybrid, a composite node, first directly request the WINS server for name resolution NetBIOS name resolution, if no response is received, NetBIOS name resolution is performed by broadcasting.

By default, the node type of the Microsoft operating system is broadcast or composite. If no WINS server is configured, it is a broadcast node; if a WINS server is configured, it is a composite node. It is recommended to set the node type of NetBIOS to Hybrid

【Configuration Example]】 1: Set the NetBIOS node of the Microsoft DHCP client as a composite node:

```
AC-FS(dhcp-config)# netbios-node-type h-node
```

【Verification】 It can be seen that the configuration is successful through show run.

【Prompt Information】-

【Common Mistake】-

3.49 network

To define the network number and netmask of the DHCP address pool, use the DHCP address pool configuration command network; To advertise the network number and netmask of the DHCP address pool configured on the thin AP, you can configure it in the ap-config/or ap-group mode of the AC.

network command.

network network-number net-mask [low-ip-address high-ip-address]

The no form can delete the definition;

Delete definitions in AC's ap-config or ap-group mode;

no network

Restore default value, AC's ap-config or ap-group does not support.

defaut network

【Parameter Description】

Parameter	Description
network-number	IP address network number of the DHCP address pool.
net-mask	The IP address netmask of the DHCP address pool. If no mask is defined, it defaults to the natural netmask.

【Default Configuration】 By default, the network number and network mask are not defined.

【Command Mode】 DHCP address pool configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to Server configuration; it defines the subnet and mask of the new address pool, and provides an address space for the DHCP server that can be allocated to clients. All addresses in the address pool may be assigned to clients unless address exclusion is configured. DHCP allocates addresses in the address pool in order. If the address is already in the DHCP binding table or it is detected that the address already exists in the network segment, the next address is checked until a valid address is allocated. Use the show ip dhcp binding command to check the address assignment, and use the show ip dhcp conflict command to check the address conflict.

【Configuration Example]】 1: The network number that defines the DHCP address pool is 192.168.12.0 and the mask is 255.255.255.240

```
AC-FS(dhcp-config)# network 192.168.12.0 255.255.255.240
```

2: The AC advertises that the AP has defined the network number of the DHCP address pool as 192.168.12.0 and the mask as 255.255.255.240.

```
AC-FS(config)# ap-group default
AC-FS(config-group) # network 192.168.12.0 255.255.255.240
```

【Verification】 It can be seen that the configuration is successful through show run.

【Prompt Information】 1: Configure an illegal address

```
AC-FS(dhcp-config)#network 238.5.5.5 255.0.0.0
238.5.5.5 / 255.0.0.0 is an invalid network
```

【Common Mistake】 1. Configure a non-unicast address

3.50 next-server

To define a list of startup servers that the DHCP client needs to access during startup, use the DHCP address pool configuration command next-server next-server ip-address [ip-address2…ip-address8]

The no form removes the definition of the startup server list.

no next-server

Restore Defaults.

defaut next-server

【Parameter Description】

Parameter	Description
ip-address	Defines the IP address of the boot server, usually a TFTP server. Requires at least one.
ip-address2…ip-address8	(Optional) Up to 8 boot servers can be configured.

【Default Configuration】 No Default Configuration.

【Command Mode】 DHCP address pool configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to Server configuration; when defining multiple startup servers, the priority written in the front is higher, and the DHCP client will select the next startup server only if the communication with the first startup server fails.

【Configuration Example]】 1: The boot server 192.168.12.4 is specified for the DHCP client.

```
AC-FS(dhcp-config)# next-server 192.168.12.4
```

【Verification】 It can be seen that the configuration is successful through show run.

【Prompt Information】 1: Configure an illegal address.

```
AC-FS(dhcp-config)# next-server 238.5.5.5
% Error: ip address(238.5.5.5) is invalid!
```

【Common Mistake】 1. Configure a non-unicast address.

2. Configure more than 8 server address lists.

3.51 option

To configure DHCP server options, use the DHCP address pool configuration command option.

option code { ascii string | hex string | ip ip-address }

The no form can delete the definition of option.

no option

Restore Defaults.

defaut option

【Parameter Description】

Parameter	Description
code	Defining DHCP option codes.
ascii string	define an ASCII string.
hex string	define hexadecimal string.
ip ip-address	Define a list of IP addresses.

【Default Configuration】 No Default Configuration.

【Command Mode】 DHCP address pool configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to Server configuration; DHCP provides a mechanism that allows configuration information to be transmitted to hosts in a TCP/IP network. The DHCP packet has a special option field, which is variable and can be defined by the user according to the actual situation. The DHCP client must be able to receive DHCP packets that carry at least 312 bytes of option information. In addition, the fixed data field in the DHCP message is also called an option. For the definition of the current DHCP option, see the RFC 2132 document.

【Configuration Example]】 1: Defines option code 19, which determines whether the DHCP client enables IP packet forwarding. 0 means disable IP packet forwarding; 1 means enable IP packet forwarding. The following configuration enables the DHCP client to enable IP packet forwarding.

```
AC-FS(dhcp-config)# option 19 hex 1
```

2: Option code 33 is defined, this option provides static routing information to the DHCP client, and the DHCP client will install two static routes:

```
AC-FS(dhcp-config)# option 33 ip 172.16.12.0 192.168.12.12 172.16.16.0 192.168.12.16
```

【Verification】It can be seen that the configuration is successful through show run.

【Prompt Information】 1: Configure an illegal static route address.

```
AC-FS(dhcp-config)#option 56 ip 2.2.2.2 225.5.5.5
% Error: ip address 225.5.5.5 is not valid!
```

2: Configure illegal hexadecimal string.

```
AC-FS(dhcp-config)#option 253 hex abcdef_
% DHCP could not parse the hexadecimal string. Check character 6 (_).
```

【Common Mistake】 15. Configure non-unicast address.

16. Configure more than 8 static routing addresses.

17. Configure an illegal hexadecimal string.

3.52 pool-status

In FS Wireless products, a new command has been added to configure whether the DHCP address pool is enabled. Through the configuration command, the corresponding address pool service can be enabled or disabled. The command does not provide the no form.

pool-status {enable | disable}

【Parameter Description】

Parameter	Description
enable	enable address pool.
disable	disables the address pool.

【Default Configuration】 After the address pool is configured, the address pool is automatically enabled.

【Command Mode】 DHCP address pool configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to Server configuration; in using DHCP server, you can use this command to temporarily disable or enable the corresponding address pool.

【Configuration Example】 1: Disable the address pool.

```
AC-FS(dhcp-config)# pool-status disable
```

【Verification】 It can be seen that the configuration is successful through show run

【Prompt Information】 -

【Common Mistake】 -

3.53 relay agent information

To enter the Option82 matching information configuration mode in the global CLASS, use the relay agent information command in the global CLASS configuration mode, the no form of this command can delete all Option82 matching information of the CLASS.

relay agent information

no relay agent information

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】-

【Command Mode】 Global CLASS configuration mode.

【Usage Guide】 This command belongs to Server configuration;

Execute this command to enter the Option82 matching information configuration mode, which is displayed as:

AC-FS (config-dhcp-class-relayinfo)#

In this configuration mode, you can configure the class to match multiple Option82 information.

【Configuration Example]】 1: Configure a global CLASS and enter the Option82 matching information configuration mode.

AC-FS(config)# ip dhcp class myclass

```
AC-FS(config-dhcp-class)# relay agent information
AC-FS(config-dhcp-class-relayinfo)#
```

【Verification】It can be seen that the configuration is successful through show run

【Prompt Information】-

【Common Mistake】-

3.54 relay-information hex

In the Option82 information configuration mode under the global CLASS, configure the matching information of option82 and call relay-information hex command, the no form of the command can delete a matching message.

relay-information hex aabb.ccdd.eeff… [*]

no relay-information hex aabb.ccdd.eeff… [*]

【Parameter Description】

Parameter	Description
aabb.ccdd.eeff… [*]	Option82 matching information in hexadecimal, * represents incomplete matching, only the front part needs to be matched Points can indicate that the match is passed, and no * indicates that an exact match is required.

【Default Configuration】 -

【Command Mode】 Global CLASS configuration mode.

【Usage Guide】 This command belongs to Server configuration.

【Configuration Example]】 1: Configure a global CLASS to match multiple option82 information.

```
AC-FS(config)# ip dhcp class myclass AC-FS(config-
dhcp-class)# relay agent information
AC-FS(config-dhcp-class-relayinfo)# relay-information hex 0102256535 AC-
FS(config-dhcp-class-relayinfo)# relay-information hex 010225654565 AC-
FS(config-dhcp-class-relayinfo)# relay-information hex 060225654565
AC-FS(config-dhcp-class-relayinfo)# relay-information hex 060223*
```

【Verification】 It can be seen that the configuration is successful through show run.

【Prompt Information】 -

【Common Mistake】 -

3.55 release-dhcp

Configuring the DHCP Client to Actively Release the Dynamically Applied IP Address.

release-dhcp type number

【Parameter Description】

Parameter	Description
class-remark	The information that identifies the CLASS, which can be a string with spaces in between.

【Default Configuration】 -

【Command Mode】 Privileged user mode.

【Default Level】 14

【Usage Guide】 This command belongs to the client configuration; this command is used to release the IP address dynamically obtained under the interface. After the interface address is released, you need to use the renew-dhcp command to restore the dynamic address or no change the configuration to re-initiate the application.

【Configuration Example]】 1: Release the dynamic address obtained by interface vlan 100.

```
AC-FS# release-dhcp vlan 100
```

【Prompt Information】 -

【Common Mistake】 -

3.56 remark

To configure the identification information of Description of the CLASS in the global CLASS.

remark class-remark

no form can delete the identification information.

no remark

【Parameter Description】

Parameter	Description
class-remark	The information that identifies the CLASS, which can be a string with spaces in between.

【Default Configuration】-

【Command Mode】 Global CLASS configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to Server configuration;

【Configuration Example]】 1: Configure a global CLASS identification information.

```
AC-FS(config)# ip dhcp class myclass
AC-FS(config-dhcp-class)# remark used in #1 build
```

【Verification】 It can be seen that the configuration is successful through show run.

【Prompt Information】-

【Common Mistake】-

3.57 renew-dhcp

Configure the DHCP Client to actively update the dynamically requested IP address.

renew-dhcp type number

【Parameter Description】

Parameter	Description
type	Interface Type.
number	interface number.

【Default Configuration】 -

【Command Mode】 Privileged user mode.

【Default Level】 14

【Usage Guide】 This command belongs to Client configuration; this command is used to update the IP address dynamically obtained under the interface

【Configuration Example]】1: Update the dynamic address obtained by interface vlan 100.

```
AC-FS# renew-dhcp vlan 100
```

【Prompt Information】 -

【Common Mistake】 -

3.58 service dhcp

To enable the DHCP server and relay agent features on the device, use the global configuration command service dhcp.

To advertise the DHCP server and relay agent feature on thin APs, configure the service dhcp command in the AC's ap-config/or ap-group mode.

service dhcp

The no form can turn off the DHCP server and relay agent features;

Or disable the AP's DHCP service and relay code feature in the AC's ap-config/or ap-group mode.

no service dhcp

Restore default value, AC's ap-config or ap-group does not support.

defaut service dhcp

【Parameter Description】

Parameter	Description
type	Interface Type.

【Default Configuration】 This command belongs to Server configuration; DHCP server and relay agent features are disabled by default.

【Command Mode】 Global configuration mode, ap-config/ap-group mode

【Default Level】 14

【Usage Guide】 The DHCP server can automatically assign IP addresses to clients, and provide network configuration information such as DNS server addresses and default gateway addresses. The DHCP relay feature can forward DHCP requests to other servers, and forward the returned DHCP response packets to the DHCP client, acting as a DHCP message relay.

Conflict between DHCP function and other functions may occur on some products. For specific problems, please refer to the detailed description of the relevant product and the Prompt Information of the configuration failure.

【Configuration Example]】 1: The device enables the DHCP server and relay features.

```
AC-FS(config)# service dhcp
```

2: The AC advertises that the AP has the DHCP server and relay features enabled.

```
AC-FS(config)# ap-group default
AC-FS(config-group) # service dhcp
```

【Verification】 It can be seen that the configuration is successful through show run

【Prompt Information】 -

【Common Mistake】 -

3.59 show dhcp lease

Display lease information obtained by DHCP clients.

show dhcp lease

【Parameter Description】

Parameter	Description
type	Interface Type.

【Default Configuration】 No default behavior.

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】 This command belongs to the client configuration; it displays the relevant information of the ip address applied as the client.

【Configuration Example】 1: Display the lease information obtained by the DHCP client.

```
AC-FS# show dhcp lease
Temp IP addr: 192.168.5.71 for peer on Interface: FastEthernet0/0
Temp  sub net mask: 255.255.255.0
DHCP Lease server: 192.168.5.70, state: 7 Bound
DHCP transaction id: 337beed
Lease: 600 secs, Renewal: 300 secs, Rebind: 525 secs
Temp default-gateway addr: 192.168.5.1
Next timer fires after: 00:04:29
Retry count: 0   Client-ID: 0100d0f82233e347696761626974457468657 26E6574302F31
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

3.60 show ip dhcp binding/

Display DHCP address binding.

show ip dhcp binding [ip-address]

【Parameter Description】

Parameter	Description
ip-address	(Optional) Display only the bindings of the specified IP address. By default all binding information is displayed.

【Default Configuration】 No default behavior.

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】 This command belongs to Server configuration; if no IP address is defined, the binding status of all addresses will be displayed. If an IP address is defined, only the bindings of that IP address will be displayed.

【Configuration Example】1: Display DHCP address binding.

```
AC-FS# show ip dhcp binding
Total number of clients : 4
Expired clients          : 3
Running clients  : 1

IP address         Hardware address        Lease expiration            Type
```

20.1.1.1 2000.0000.2011 000 days 23 hours 59 mins Automatic The meaning of each field of the displayed result is explained as follows:

IP address	The IP address assigned to the DHCP client.
Hardware address	Hardware address of the DHCP client.
Lease expiration	Lease expiry time. Infinite means there is no time limit; IDLE means the currently idle address, the unprecedented reason may be that it has expired without renewing the ancestor or the DHCP client actively released it.
Type	Address binding type. Automatic means automatic allocation; Manual means manual allocation.

【Verification】-

【Prompt Information】-

【Common Mistake】-

3.61 show ip dhcp conflict

Display conflict records for DHCP servers.

show ip dhcp conflict

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 No default behavior.

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】 This command belongs to Server configuration; this command can display the list of conflicting addresses detected by the DHCP server

【Configuration Example】1: Display the conflict record of the DHCP server

```
AC-FS# show ip dhcp conflict
IP address  Detection Method
192.168.12.1                    Ping
```

The meaning of each field of the displayed result is explained as follows:

IP address	An IP address that cannot be assigned to a DHCP client.
Detection Method	Conflict detection method.

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

3.62 show ip dhcp database

Display the operation of the database backup function of DHCP SERVER.

show ip dhcp database

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 No default behavior.

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】 This command belongs to Server configuration; this command can display the information of DHCP database.

【Configuration Example】1: Display DHCP database information.

```
AC-FS#show ip dhcp database
Enable           :No
Status           :ready
Save File        :Default
Successs  :0
Failures         :0
Interval Time    :86400
```

The meaning of each field of the displayed result is explained as follows:

Enable	Whether to enable the database data function for data recovery when the device is restarted.
Status	data recovery status.
Save File	Data save file path.
Successs	Number of successful data saves.
Failures	Failed to save data.
Interval Time	Data save interval.

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

3.63 show ip dhcp history

Display DHCP historical lease records

show ip dhcp history

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 No default behavior.

【Command Mode】 Privileged user mode.

【Default Level】 14

【Usage Guide】 This command belongs to Server configuration; this command can display lease information that has been allocated by DHCP.

【Configuration Example】1: Display lease information that has been assigned by DHCP.

```
AC-FS#show ip dhcp history
Expired clients            : 3
IP address        Hardware address       Lease expiration           Vlan/Relay
10.1.1.5.....2222.abcd.47ac          IDLE                         4097
10.1.1.4.....2222.abcd.47ae          IDLE                         4097
10.1.1.3.....2222.abcd.47ad          IDLE                         4097
Running clients                :0
```

The meaning of each field of the displayed result is explained as follows:

IP address	The IP address assigned to the HCP client.
Hardware address	MAC address of the DHCP client
Lease expiration	Lease expiry time. Infinite means there is no time limit; IDLE means the currently idle address, the unprecedented reason may be that it has expired without renewing the ancestor or the DHCP client actively released it.
Vlan/Relay	When the DHCP client applies for an address to the DHCP Server through the DHCP Relay, it will display the address of the DHCP Relay; otherwise, it will display the port ifindex that received the DHCP message.

【Verification】-

【Prompt Information】-

【Common Mistake】-

3.64 show ip dhcp identifier

Displays the ID and address usage of the DHCP server address pool.

show ip dhcp identifier

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 No default behavior.

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】 This command belongs to Server configuration; this command can display the ID and address usage of the DHCP server address pool. The displayed address pool ID can be used to form the OID of the MIB in order to access specific contents of a specific address pool.

【Configuration Example】 1: Display the ID of the DHCP server address pool.

```
AC-FS# show ip dhcp identifier
Pool  name     Identifier       Total      Distributed  Remained
-----------  -----------  -----------  -----------  --------
wwp          597455782    65533        0            65533
```

The meaning of each field of the displayed result is explained as follows:

Pool name	The name of the address pool.
Identifier	Address pool ID.
Total	The total number of address pools available for allocation in the address pool.
Distributed	The number of addresses allocated.
Remained	Includes the number of unallocated and reusable remaining addresses.

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

3.65 show ip dhcp pool

Displays information such as the address pool usage and utilization of the DHCP server.

show ip dhcp pool [poolname]

【Parameter Description】

Parameter	Description
poolname	(Optional) View only the address pool information of the specified name. By default, all address pool configurations are displayed.

【Default Configuration】 No default behavior.

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】 This command belongs to Server configuration; this command can display the DHCP server address pool usage and address utilization and other information.

【Configuration Example]】 1: Display the address pool usage and utilization of the DHCP server and other information

```
AC-FS# show ip dhcp pool AC-
FS#sh ip dh pool
Pool  name        Total      Distributed  Remained   Percentage
____________  ____________  ____________  ________  ____________

net20         253           11            242        4.34782
Test          0             0             0          0.00000
```

The meaning of each field of the displayed result is explained as follows:

Pool address	The name of the address pool.
Total	The total number of address pools available for allocation in the address pool.

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

3.66 show ip dhcp relay-statistics

Displays various statistics for the DHCP server.

show ip dhcp relay-statistics

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 No default behavior.

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】 This command belongs to Relay configuration.

【Configuration Example】 1. Display various statistics of DHCP-Relay.

```
AC-FS#show ip dhcp relay-statistics
Cycle mode                0

Message
Count Discover
0 Offer
0 Request
0
Ack                       0
Nak                       0
Decline                   0
Release                   0
Info                      0
Bad                       0
Direction
Count Rx client
0
Rx client uni             0
Rx client bro             0
Tx client                 0
Tx client uni             0
Tx client bro             0
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

3.67 show ip dhcp server detect

Display a list of fake servers detected by DHCP.

show ip dhcp server detect

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 No default behavior.

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】 This command belongs to Server configuration.

【Configuration Example】 1. Display the list of fake servers detected by DHCP Server.

```
AC-FS#show ip dhcp server detect
The DHCP Server information:
Server IP = 10.1.10.40, DHCP server interface = GigabitEthernet 0/1
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

3.68 show ip dhcp server statistics

Displays various statistics for the DHCP server.

show ip dhcp server statistics

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 No default behavior.

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】 This command belongs to the server configuration; this command can display the current statistics of the DHCP server.

【Configuration Example】 1. Display various statistics of DHCP server.

```
AC-FS# show ip dhcp server statistics
Address pools              2
Lease  counter             4
Active   Lease   Counter   0
Expired   Lease   Counter   4
Malformed   messages       0
Dropped messages           0

Message
Received BOOTREQUEST
216 DHCPDISCOVER
33 DHCPREQUEST                  25
DHCPDECLINE                    0
DHCPRELEASE                    1
DHCPINFORM                     150

Message
Sent BOOTREPLY
16 DHCPOFFER
9 DHCPACK
7
```

```
DHCPREQTIMES
0 DHCPREQSUCTIMES 0
DISCOVER-PROCESS-ERROR 0
LEASE-IN-PINGSTATE 0 NO-
LEASE-RESOURCE 0 SERVERID-
NO-MATCH  0
-----------------------------------------

recv                          0
send                          0
```

The meaning of each field of the displayed result is explained as follows:

Address pools	number of address pools.
Automatic bindings	The number of automatic address bindings.
Manual bindings	The number of manual address bindings.
Expired bindings	The number of expired address bindings.
Malformed messages	The number of abnormal packets received by DHCP.
Message Received or Sent	The number of each type of packet received and sent by the DHCP server.

DHCPREQTIMES	The total number of request packets received by DHCP.
DHCPREQSUCTIMES	Number of packets successfully processed for requests received by DHCP.
DISCOVER-PROCESS-ERROR	The number of errors in processing DISCOVER packets received by DHCP.
LEASE-IN-PINGSTATE	The number of leases currently in the PING detection state.
NO-LEASE-RESOURCE	Number of full address pools with no addresses to allocate.
recv	The total number of received DISCOVER, REQUEST, INFORM messages.
send	Statistics on the number of response packets that should have been sent.

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

3.69 show ip dhcp socket

Displays the connector index used by the DHCP server.

show ip dhcp socket

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example】 1: Display the socket index used by the DHCP server.

```
AC-FS#show ip dhcp socket
dhcp socket = 47.
```

【Prompt Information】 -

【Platform Description】 -

3.70 show ip dhcp state ssid

Display DHCP address binding based on wireless SSID.

show ip dhcp state ssid [ssid]

【Parameter Description】

Parameter	Description
ssid	The name of the SSID to retrieve.

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】 In the case of specifying SSID, it will display the address bindings associated with the SSID, and if the SSID is not specified, it will display all address bindings.

【Configuration Example]】 1: Display SSID-based DHCP address binding.

```
AC-FS#show ip dhcp state ssid wlan_free
SSID                                IP   address                Hardware   address    State              Expiratior
Type



wlan_free  192.168.110.2            0cd6.bd90.4f07        ACTIVE        000 days 23 hours 48 mins   Automatic
AC-FS#show ip dhcp state ssid
SSID                    IP address            Hardware address   State          Expiration                    Type



wlan_free........192.168.110.2      0cd6.bd90.4f07      ACTIVE      000 days 23 hours 48 mins
Automatic
```

`

【Prompt Information】 -

【Platform Description】 -

3.71 update arp

To add trusted ARP when DHCP assigns addresses, use the DHCP address pool configuration command update arp.

update arp

The no form indicates that DHCP does not add trusted ARP when assigning addresses.

no update arp

Restore Defaults.

defaut update arp

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 By default, DHCP does not add trusted ARP when assigning addresses..

【Command Mode】 DHCP address pool configuration mode

【Default Level】 14

【Usage Guide】 This command belongs to Server configuration. After the address pool is configured with update arp, DHCP will add trusted ARP when assigning addresses from the address pool. Trusted ARP.

The priority is higher than that of dynamic ARP and will not be overwritten by dynamic ARP.

【Configuration Example]】 1: Add trusted ARP when DHCP assigns addresses.

```
AC-FS(dhcp-config)# update arp
```

【Verification】 It can be seen that the configuration is successful through show run.

【Prompt Information】 -

【Common Mistake】 -

4 DNS

4.1 clear host

Clear the dynamic hostname buffer table.

clear host [* | host-name]

【Parameter Description】

Parameter	Description
host-name	You can delete a specified dynamic domain name buffer.
*	Deltes all dynamic domain buffers.

【Command Mode】 Privilege User Mode

【Default Level】 14

【Usage Guide】 Mapping records in the hostname buffer table, with two sources:

1. Static configuration via the ip host;

2. Dynamic learning through the DNS. Performing this command removes the hostname record that is currently dynamically learned through the DNS.

【Configuration Example】 1: In the following configuration, all dynamically learned mapping records in the hostname-IP address buffer table are removed.

```
AC-FS(config)#clear host *
```

【Prompt Information】 -

【Platform Description】 -

4.2ip domain-lookup

Start the DNS for domain name resolution.

ip domain-lookup

Turn off the DNS domain name resolution function.

no ip domain-lookup

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 The default is to open the DNS domain name resolution function.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command is a switch on DNS domain name resolution function and execute this command, start DNS for domain name resolution.

【Configuration Example】 1: Turn off the DNS domain name resolution function.

```
AC-FS(config)# no ip domain-lookup
```

【Verification】View the configuration through the show run, and no ip domain-lookup configuration exists.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

4.3 ip host

Handconfigure the mapping of the hostname and IP addresses.

ip host host-name ip-address

Delete the host list.

no ip host host-name ip-address

【Parameter Description】

Parameter	Description
host-name	The host name of the device.

ip-address	The IP address of the device.

【Default Configuration】 -

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】

【Configuration Example】 1: The static configuration www.test.com domain name is 192.168.5.243

```
AC-FS(config)# ip host www.test.com 192.168.5.243
```

【Verification】 show run View the configuration, and the configured command exists show hosts View the current domain name and IP correspondence, with the configured domain name and IP correspondence table items.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

4.4 ip name-server

Configure the IP address of the domain name server.

ip name-server{ ip-address }

Delete the configured domain name server.

no ip name-server [ip-address]

【Parameter Description】

Parameter	Description
ip-address	The IP address of the domain name server

【Default Configuration】 The domain name server is not configured by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Only a domain name server is configured for dynamic domain name resolution.

Add the IP address of the DNS Server.Each time this command is executed, the device adds a DNS Server.When unable to get from the first Server.

When acquiring a domain name, the device tries to send DNS requests to several subsequent Server s until the correct response is received.

The system supports up to 6 servers. When you delete a DNS Server, if you specify the ip-address parameter, delete only the specified server, otherwise delete all DNS server addresses.

【Configuration Example】 1: Configure the IPv4 domain name server

```
AC-FS(config)# ip name-server 192.168.5.134
```

【Verification】 show run View the configuration, and the configured command exists.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

4.5ip name-server white-list

Configure the DNS server IP.

ip name-server white-list [wlan wlan-id] ip-address

Removes the DNS Server IP.

no ip name-server white-list [wlan wlan-id] ip-address

【Parameter Description】

Parameter	Description
wlan-id	The ID value of the WLAN.
ip-address	The IP address of the domain name server.

【Default Configuration】 The DNS server is not configured by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 All DNS messages are filtered without a legitimate DNS server.

Only address settings for the IPv4 DNS server are currently supported, with up to 6 DNS server addresses configured.

【Configuration Example】 1: Configure the DNS server.

```
AC-FS(config)# ip name-server white-list 192.168.5.134
```

【Verification】 Show run View the configuration, and the configured command exists.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

4.6 ip name-server white-list enable

Start the DNS whitelist feature.

ip name-server white-list [wlan wlan-id] enable

Turn off the configured domain name server.

no ip name-server white-list [wlan wlan-id] enable

【Parameter Description】

Parameter	Description
wlan-id	The ID value of the WLAN

【Default Configuration】 The DNS whitelist function is turned off by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 After the device turns on the DNS whitelist check function, check the DNS message flowing through the device and intercept the message that access the illegal DNS server. All DNS messages are filtered without a legitimate DNS server configured.
You can enable DNS whitelist functions based on WLAN or globally and configure legitimate DNS server lists. When WLAN-enabled DNS whitelist functions is enabled, DNS messages received from WLAN do not access the IP address of the WLAN-based legitimate DNS server, the message will be discarded directly, and no longer match the global DNS whitelist configuration.

【Configuration Example]】 1: turn on the DNS whitelist function.

```
AC-FS(config)# ip name-server white-list enable
```

【Verification】 show run View the configuration, and the configured command exists.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

4.7 show hosts

Displays the configuration information for the DNS.

show hosts [hostname]

【Parameter Description】

Parameter	Description
hostname	View the specified domain name. View all of the domain name information by default.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Displays the relevant configuration information for the DNS.

【Configuration Example】 1: View all of the domain name information.

```
AC-FS# show hosts
Name servers are:
```

```
192.168.5.134 static

Host                type          Address                TTL(sec)
switch               static         192.168.5.243 ----------
www.AC-FS.com    dynamic        192.168.5.123                  126
```

Field interpretation:

Field	interpretation
Name servers	domain name server.
Host	domain name.
type	Parse type: static resolution or dynamic resolution.
Address	The IP corresponding to the domain name.
TTL	Domain name / IP corresponds to the table item survival time.

【Prompt Information】 -

【Platform Description】 -

4.8 show ip name-server white-list

Displays the configuration information for the DNS whitelist.

show ip name-server white-list [wlan wlan-id]

【Parameter Description】

Parameter	Description
wlan-id	The ID value of the WLAN.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Displays the relevant configuration information for the DNS whitelist.

【Configuration Example】 1: View all of the domain name information

```
AC-FS# show ip name-server white-list
white-list check: enable
white-list name-server:
192.168.10.1
```

【Prompt Information】 -

【Platform Description】 -

5 FTP-Server

5.1ftp-server enable

Start the FTP server

ftp-server enable.

Restore the Default Configuration default.

ftp-server enable

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 off state.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 When the FTP server is enabled, the FTP client allows file upload or download, and both the ftp-server topdir command must be configured for the FTP client to access files on the FTP server.

【Configuration Example]】 1: Start the FTP server and restrict the client to having access to the syslog subdirectory only:

```
AC-FS(config)# ftp-server topdir /syslog
AC-FS(config)# ftp-server enable
```

2: Turn off the FTP server:

```
AC-FS(config)# no ftp-server enable
```

【Verification】1:The show ftp-server can see that the configuration is successful.

【Common Mistake】-

【Platform Description】 -

5.2ftp-server login timeout

Configure a valid time for the FTP session landing.

ftp-server login timeout time

Recovery idle time using this command as no is the default value (2 min).

no ftp-server login timeout

Restore the Default Configuration.

default ftp-server login timeout

【Parameter Description】

Parameter	Description
time	Idle time limit (unit: minutes; range: 1-30).

【Default Configuration】 The default time limit is 2 minutes.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 The login valid time refers to the maximum online time when the user authenticates his account and password each time after the user establishes a link. If the user does not conduct user password authentication again during this valid time, ensuring that other users can log in.

【Configuration Example】 1: The following shows how to configure the idle time limit of 5 minutes:

```
AC-FS(config)# ftp-server login timeout 5
```

2: The following demonstrates how to restore idle time is the default (10 minutes):

```
AC-FS(config)# no ftp-server login timeout
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.3 ftp-server login times

Configure the valid number of landing times for an FTP session.

ftp-server login times time

Recovery of no with this command to default (3 times).

no ftp-server login times

Restore the Default Configuration.

default ftp-server timeout

【Parameter Description】

Parameter	Description
time	Idle time limit (range: 1-10).

【Default Configuration】 The default number is 3 times

【Command Mode】Global configuration mode

【Default Level】 14

【Usage Guide】 The effective number of sessions refers to the maximum number of times that users can authenticate their account and password during an FTP session. The default setting is to 3 times, where the session is aborted when accumulating three incorrect username or password is entered, allowing other users to go online.

【Configuration Example】 1: The following shows how to configure the idle time limit of 5 minutes:

```
AC-FS(config)# ftp-server login times 5
```

2: The following demonstrates how to restore the idle time to the default value (3 times):

```
AC-FS(config)# no ftp-server login times
```

【Verification】

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

5.4ftp-server topdir

Limit the range of directories where FTP clients can perform file read and write operations.

ftp-server topdir directory

Use the command in its no form to completely prohibit client access to any files on the FTP server.

no ftp-server topdir

Restore the Default Configuration.

default ftp-server topdir

【Parameter Description】

Parameter	Description
directory	Top-level directory where the FTP client can operate.

【Default Configuration】 No top-level directory settings by default (reading and writing any directories are not allowed).

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 The FTP server top directory limits the range of file directories you can access after client login. The top-level directory must be correctly specified to let the FTP clients access the files on the FTP server If the command is not configured, the FTP client will not be able to access any files or directories on the server.

【Configuration Example]】 1: The following demonstrates how to start the FTP server and restrict client access to the syslog subdirectory.

```
AC-FS(config)# ftp-server topdir /syslog
AC-FS(config)# ftp-server enable
```

2: The following example demonstrates how to unconfigure the root directory.

```
AC-FS(config)# no ftp-server topdir
```

【Verification】 1: The show ftp-server can see that the configuration is successful.

【Prompt Information】 1: The access directory is not configured.

```
%FTPSRV-4-USER: Haven't config topdir!
```

2: Configure a directory that does not exist

```
AC-FS(config)#ftp-server topdir ab
folder /ab don't exist!
```

【Common Mistake】 1. Configure an illegal directory.

2. The directory is not configured.

【Platform Description】 -

5.5ftp-server timeout

Configure the idle time limit for an FTP session (Session idle timeout).

ftp-server timeout time

Recovery idle time in the no form of this command is the default value (10 min).

no ftp-server timeout

Restore the Default Configuration.

default ftp-server timeout

【Parameter Description】

Parameter	Description
time	Idle time limit (unit: minutes; range: 1-3600).

【Default Configuration】 The default time limit is 10 minutes.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Configure the idle time limit for the FTP session. If the current session does not operate at the specified time limit (session idle), the FTP server can consider the connection invalid, and the idle time of disconnecting the user is the time between an FTP session and the completion of the last FTP operation and the start of the next FTP operation. The server calculates the session idle time from 0 after an FTP command service is completed (if a file is transferred) and stops counting the session idle time when the next command arrives. So the configuration of the session idle time limit does not have any impact on some time-consuming file transfer operations.

【Configuration Example】 1: The following shows how to configure the idle time limit of 5 minutes:

```
AC-FS(config)# ftp-server timeout 5
```

2: The following demonstrates how to restore idle time is the default (10 minutes):

```
AC-FS(config)# no ftp-server timeout
```

【Verification】 1.The show ftp-server can see that the configuration is successful.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

5.6ftp-server username password

Configure the login username and password for the FTP server.

ftp-server username username password [type] password

Unconfigure the user name by using the no form of the command.

no ftp-server username username

Restore the Default Configuration.

default ftp-server username username

【Parameter Description】

Parameter	Description
username	Log on to the username.
password	Login password.

【Default Configuration】 By default, there is no username, and no password.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Configure the user name that the client needs to provide when logging in to the FTP server. When logging in, the client needs to provide both the correct user name and password to log in.

The maximum length of the username is 64 characters, and no spaces are allowed. Username can be composed of English letters, half-width numbers and half-width symbols. The FTP server can only be configured with a maximum of 10 users.

The password must contain letters or numbers, and spaces before and after the password can be ignored; spaces in the middle of the password are part of the password.

The minimum length of plaintext passwords is 1 character and the maximum length is 25 characters; the minimum length of ciphertext passwords is 4 characters and the maximum length is 52 characters.

The FTP server must be configured with a login username and login password to authenticate client connections, and the password and user are paired one by one. The FTP server does not support anonymous user login, if the user name configuration is cleared, the client will not be able to authenticate to the server.

【Configuration Example】Example 1: The following demonstration shows how to configure the username as user:

```
AC-FS(config)# ftp-server username user password pass
```

Example 2: The following example demonstrates how to cancel the username configuration:

```
AC-FS(config)# no ftp-server username user
```

【Verification】1:The show ftp-server visible configuration was successful.

【Prompt Information】 1:No user name is configured, and the user tries to connect.

```
%FTPSRV-4-USER: Haven't config username!
```

2. The configuration user name is too lon.

```
AC-FS(config)#$sssssssssssssssssssssssssssssssssssddddddddddddddd
Username abcdefghijklnn, sssssssssssssssssssssssssssssssssssddddddddddddddd
is NULL or too long, max length is 64.
```

3: The password is not configured on the Server side, and the user tries to connect.

```
%FTPSRV-4-PASS: Haven't config password!
```

4: Configuring the ciphertext password length is too short.

```
AC-FS(config)#ftp-server username user password 7 2
Invalid encrypted password, min length is 4, max length is 52.
```

5: Configure the clear text password is too long.

```
AC-FS(config)#ftp-server username user password abcdefghijklmnopqrstuvwxyz
% Password is too long, max length is 25
```

【Common Mistake】 1. The configuration user name contains illegal characters or is too long.

2. Try to connect without user name.

3. The user does not have the password configured.

4. Configure the password length is too short or too long.

5. Enter an illegal password.

【Platform Description】 -

5.7 show ftp-server

Displays the relevant status information for the FTP server.

show ftp-server

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 -

【Command Mode】 Privilege User Mode

【Default Level】 14

【Usage Guide】 Displays the relevant status information for the FTP server, including:

1. When the server is started.

2. Whither to establish a control connection (and display the relevant IP, Port).

3. Whither to establish a data connection (and show whether the active or passive mode, and the associated IP, Port).

4. The Current File Transfer type.

5. Server login username, password (with configuration only).

6. Server top-level directory.

【Configuration Example】1: The following example shows how to view the relevant status information of the FTP server

```
AC-FS# show ftp-server
ftp-server information
=====================================
enable : Y
topdir : /
timeout: 20min
username config : Y
password config : Y
type:  BINARY
control connect : Y
ftp-server: ip=192.167.201.245 port=21
ftp-client: ip=192.167.201.82 port=4978
port data connect : Y
ftp-server: ip=192.167.201.245  port=22
```

```
ftp-client: ip=192.167.201.82  port=4982
passive data connect : N
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6 FTP Client

6.1 default ftp-client

Restore the FTP Client Default Configuration.

default ftp-client

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to restore the FTP Client to Default Configuration, that is, the data connection is in the passive (PASV) mode, the file transfer is in the binary (BINARY) mode, and the client source IP address is not bound.

【Configuration Example】1: The FTP Client is restored to Default Configuration.

```
AC-FS(config)# default ftp-client
```

【Verification】1: Use the show run command to view any configuration information about ftp-client.

【Prompt Information】 1: The configuration is successful without any prompt.

【Common Mistake】-

【Platform Description】 -

6.2ftp-client ascii

Use text (ASCII) for FTP transfers.

ftp-client ascii

Cancel the text transmission method and use the binary transmission method.

no ftp-clientascii

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 By default, the FTP transfer mode is BINARY.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Configure to use text (ASCII) mode for FTP transmission.

```
AC-FS(config)# ftp-client ascii
```

2: Configure to use text (BINARY) mode for FTP transfer.

```
AC-FS(config)# no ftp-client ascii
```

【Verification】1: Use the show run command to view the ftp-client ascii configuration.

【Prompt Information】 1: The configuration must be successful, and no prompt will appear.

【Common Mistake】-

【Platform Description】 -

6.3ftp-client port

Configure FTP to use active (PORT) mode for data connection.

ftp-client port

Revert to passive mode.

no ftp-client port

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 By default, the FTP connection is passive (PASV) mode

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to set the connection mode to active, that is, the server takes the initiative to connect to the client.

【Configuration Example]】 1: Configure FTP to use active (PORT) mode for data connection.

```
AC-FS(config)# ftp-client port
```

2: Configure the FTP connection as passive (PASV) mode.

```
AC-FS(config)# no ftp-client port
```

【Verification】 1: Use the show run command to view the ftp-client port configuration.

【Prompt Information】 1: The configuration must be successful, and no prompt will appear.

【Common Mistake】-

【Platform Description】 -

6.4ftp-client source

The FTP Client can bind the source IP address of the client and use this IP address to communicate with the IP address of the server.

ftp-client source {ip-address | interface}

Unbind the client source IP address.

no ftp-client source

Restore Default Configuration.

default ftp-client

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 By default, the client does not perform local IP binding, and the route is selected.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Note that when using the default command, restore the FTP Client to the Default Configuration, that is, the data connection is in the passive (PASV) mode, the file transfer is in the binary (BINARY) mode, and the client source IP address is not bound. This command replaces the ftp-client source-address {ip-address } command to configure the source interface and IP. The ftp-client source-address {ip-address } command will be automatically converted to a new command and saved.

【Configuration Example]】1: Configure the FTP Client to bind the client source IP address to 192.168.23.236.

```
AC-FS(config)# ftp-client source 192.168.23.236
```

2: Configure the FTP Client to bind the client source IP to the 2003:0:0:0::2 address.

```
AC-FS(config)# ftp-client source 2003:0:0:0::2
```

3: Configure the FTP Client vrf-name to bind the client source interface to the tenGigabitEthernet 1/0/1 interface address.

```
AC-FS(config)# ftp-client source tenGigabitEthernet 1/0/1
```

4: The no command unbinds the source IP address of the client.

```
AC-FS(config)# no ftp-client source
```

5: The FTP Client is restored to Default Configuration.

```
AC-FS(config)# default ftp-client
```

【Verification】1: Use the show run command to view the ftp-client source192.168.23.236 configuration.

2: Use the show run command to view the ftp-client source 2003:0:0:0::2 configuration.

【Prompt Information】 1: If 192.168.23.236 is not a local address, an error will be prompted; if it is, the configuration is successful and no prompt will appear.

2: If 2003:0:0:0::2 is not a local address, an error will be displayed: Bind failed: the specified source address is non-local ip; if it is, the configuration is successful and no prompt will appear.

【Common Mistake】-

【Platform Description】 -

6.5 copy ftp

Use FTP Client to download files from the server to the device.

copy ftp://username:password@dest-address [/remote-directory] / remote-file flash:[local-directory/] local-file

【Parameter Description】

Parameter	Description
username	The account name for logging in to the FTP Server, the length is limited to 32 bytes, and cannot contain characters such as ":", "@", "/" and spaces, and cannot be omitted.
password	The account password for logging in to the FTP Server, the length is limited to 32 bytes, and cannot contain ":", "@", Characters such as "/" and spaces cannot be omitted
dest-address	IP address of the accessed FTP server
remote-directory	Optional file path name on the FTP server, the length is limited to 255 bytes, spaces and Chinese characters are not supported, if it is empty, it means the current working path of the FTP server.
remote-file	The file name on the remote server, the length is limited to 255 bytes, spaces and Chinese characters are not supported.
local-directory	Optional local device folder path. If the file path is specified, it must be ensured that the folder path has been created in advance. This command does not support the automatic creation of folders; if it is empty, it means the current directory of the device, and the length is limited to 255 characters. section, spaces and Chinese characters are not supported.
local-file	The file name on the local device, the length is limited to 255 bytes, spaces and Chinese characters are not supported.

【Default Configuration】 None

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】 1: Download a file named remote-file from the root directory of the FTP Server whose username is user, password is pass, and IP address is 192.168.23.69 file to the home directory of the device, and the stored file name is local-file.

```
AC-FS# copy ftp://user:pass@192.168.23.69/root/remote-file flash:home/local-file
```

2: Upload the local-file in the home directory of the device to the root directory of the FTP Server, The file is named remote-file.

```
AC-FS# copy flash:home/local-file ftp://user:pass@192.168.23.69/root/remote-file
```

【Verification】Use dir to check whether the local-file file exists on the local device. If there is a successful download, there is no download failure.

【Prompt Information】 If the download is not successful, open debug ftp-client will prompt the corresponding error, if successful, it will prompt success.

【Common Mistake】-

【Platform Description】 -

6.6copy flash

Use FTP Client to upload files from the local device to the server.

copy flash:[local-directory/] local-file ftp://username:password@dest-address [/remote-directory] / remote-file

【Parameter Description】

Parameter	Description
username	The account name for logging in to the FTP Server, the length is limited to 32 bytes, and cannot contain characters such as ":", "@", "/" and spaces, and cannot be omitted.
password	The account password for logging in to the FTP Server, the length is limited to 32 bytes, and cannot contain ":", "@", Characters such as "/" and spaces cannot be omitted
dest-address	IP address of the accessed FTP server.
remote-directory	Optional file path name on the FTP server, the length is limited to 255 bytes, spaces

	and Chinese characters are not supported, if it is empty, it means the current working path of the FTP server.
remote-file	The file name on the remote server, the length is limited to 255 bytes, spaces and Chinese characters are not supported.
local-directory	Optional local device folder path. If the file path is specified, it must be ensured that the folder path has been created in advance. This command does not support the automatic creation of folders; if it is empty, it means the current directory of the device, and the length is limited to 255 characters. section, spaces and Chinese characters are not supported.
local-file	The file name on the local device, the length is limited to 255 bytes, spaces and Chinese characters are not supported.

【Default Configuration】 None

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】 1: From the FTP Server with user name user, password pass, and IP address 192.168.23.69, upload the local-file file in the home directory of the device to the root directory of the FTP Server, and the file name is remote-file.

```
AC-FS# copy flash:home/local-file ftp://user:pass@192.168.23.69/root/remote-file
```

【Verification】Check whether the local-file file exists in the root directory of the FTP Server. If there is a successful download, there is no download failure.

【Prompt Information】 If the upload is not successful, open debug ftp-client will prompt the corresponding error, if successful, it will prompt success.

【Common Mistake】-

【Platform Description】 -

7 TUNNEL

7.1 keepalive

Enable the keep-alive function of the GRE tunnel, and configure the interval for sending keep-alive packets and the number of retransmissions.

keepalive [seconds [retries]]

Disable the GRE tunnel keep-alive function.

no keepalive

【Parameter Description】

Parameter	Description
seconds	Interval for sending keepalive packets, in seconds. The setting range is 1 to 32767. The default is 10 seconds.
retries	Number of keepalive packet retries. If the number of retries is up and there is no response, set the protocol status of the tunnel interface to down. The value ranges from 1 to 255. The default is 3 times.

【Default Configuration】 The keep-alive function is not enabled.

【Command Mode】 Interface mode

【Default Level】 2

【Usage Guide】 The physical interface sent out by the tunnel packet is up, but there may be a problem with the line, which causes the tunnel packet to fail to reach the peer. At this time, you can enable the keep-alive function of the tunnel to detect the reachability of the tunnel interface.

【Configuration Example]】1: Create a tunnel interface.

```
AC-FS(config)# interface tunnel 1
```

2: Set the tunnel mode.

```
AC-FS(config-if)# tunnel mode ipip
```

3: Enable the keep-alive function.

```
AC-FS(config-if)# keepalive
```

【Verification】1: Use the show interface tunnel command to check whether the keep-alive function is enabled or disabled.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

7.2show interfaces tunnel

Displays an overview of the tunnel configuration. Use the following command.

show interfaces tunnel [number]

【Parameter Description】

Parameter	Description
number	Displays the overview of the tunnel corresponding to the specified number. If this Parameter is not specified, the overview of all tunnels will be displayed. Note that if a number is specified, the tunnel requirement corresponding to that number is already created.

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】 2

【Usage Guide】 Use this command to view all information about a tunnel.

【Configuration Example]】 1: View the details of tunnel 1

```
AC-FS#show interfaces tunnel 1

Tunnel source 1.1.1.2, destination 1.1.1.1, routeable
  Tunnel TOS/Traffic Class not set, Tunnel TTL 254
  Tunnel config nested limit is 0, current nested number is 0
  Tunnel protocol/transport is ipip
  Tunnel transport VPN is no set
```

Field Description:

Field	Description
Destination	The destination of the tunnel should be 0.0.0.0 which means no configuration
Tunnel source	The local address of the tunnel. If the tunnel source interface is configured, the address on the interface is taken.
Tunnel TTL	TTL or hoplimit Field corresponding to the transport protocol.
Tunnel TOS	TOS or traffic class Field corresponding to the transport protocol. Special case: If it is 0, and the transmission protocol and the payload protocol are the same, generally copy the corresponding Field of the payload protocol to the transmission protocol.
Tunnel nested-limi	The number of nested encapsulation of tunnels is limited. 6to4, 6rd, and isatap tunnels are not displayed. Other tunnels will display this Field.
Tunnel protocol/transport	The encapsulation mode of the tunnel, that is, the mode configured by tunnel mode
Key	The security key of the tunnel is set to key, only the gre tunnel will display this Field, and other tunnels will not display it.
Checksuming	Whether checksum is configured, the gre tunnel will display this Field, and other tunnels will not display it.
Tunnel VPN	The vrf to which the tunnel packet is delivered, that is, the vrf configured by the tunnel vrf

【Prompt Information】 -

【Platform Description】 -

7.3 show tunnel statistics

Displays the configurable capacity and used number of tunnels.

show tunnel statistics

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】 2

【Usage Guide】 Through this command, you can view the information about the number of configured and configurable tunnel ports of the tunnel.

【Configuration Example]】1: View the configured number of tunnel ports.

```
AC-FS#show tunnel statistics
used: 2,  limit: 1000
```

【Prompt Information】-

【Platform Description】 -

7.4 Tunnel checksum

Enable tunnel interface data integrity verification.

tunnel checksum

Disable tunnel interface data integrity verification.

no tunnel checksum

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 Disable the tunnel interface data integrity verification.

【Command Mode】 Interface mode

【Default Level】 2

【Usage Guide】 This command is only applicable to the Generic Route Encapsulation (GRE) interface. Some encapsulated protocols add a checksum that is automatically attached to the media at the end of the data packet. At this time, the tunnel interface must also perform checksum verification, and the damaged packets will be discarded directly.

【Configuration Example]】1: Create a tunnel interface.

```
AC-FS(config)# interface tunnel 1
```

2: Set the tunnel mode.

```
AC-FS(config-if)# tunnel mode gre ip
```

3: Enable data integrity verification.

```
AC-FS(config-if)# tunnel checksum
```

【Verification】1: Use the show interface tunnel command to check whether the data integrity verification function is enabled or disabled.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

7.5tunnel destination

Set the peer address of the tunnel interface.

tunnel destination ip-address

Delete the peer address.

no tunnel destination

【Parameter Description】

Parameter	Description
ip-address	Peer IP address.

【Default Configuration】 The peer address is not configured.

【Command Mode】 Interface mode

【Default Level】 2

【Usage Guide】 The peer addresses of tunnel mode ipip and tunnel mode gre ip need to be configured as IPv4 addresses.

【Configuration Example]】1: Create a tunnel interface.

```
AC-FS(config)# interface tunnel 1
```

2: Set the tunnel mode.

```
AC-FS(config-if)# tunnel mode gre ip
```

3: Set the peer address of the tunnel.

```
AC-FS(config-if)# tunnel destination 1.1.1.1
```

【Verification】 1: Use the show interface tunnel command to view the peer address of the tunnel configuration.

【Prompt Information】 1: If the set peer address is the same as the peer address of another tunnel, and the source addresses of the two tunnels are also the same, it will prompt an error.

```
%Maybe Tunnel XXX satisfy you
```

【Common Mistake】 1: The configured peer address does not match the tunnel mode. 2: The configured peer address is network unreachable.

【Platform Description】 -

7.6tunnel key

Use an integer as the tunnel's security key.

tunnel key value

Restore Default Configuration.

no tunnel key

【Parameter Description】

Parameter	Description
value	The key value of tunnel, the value range is 0- 2147483647.

【Default Configuration】 There is no key setting.

【Command Mode】 Interface mode

【Default Level】 2

【Usage Guide】If a tunnel is established without some key protection, it may be illegally invaded or bombarded by packets. The tunnel key command takes effect only in the GRE tunnel.

【Configuration Example]】1: Create a tunnel interface.

```
AC-FS(config)# interface tunnel 1
```

2: Set the tunnel mode.

```
AC-FS(config-if)# tunnel mode gre ip
```

3: Set the tunnel key.

```
AC-FS(config-if)# tunnel key 1234
```

【Verification】1: Use the show interface tunnel command to view the security key configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

7.7tunnel mode

Modify the tunnel encapsulation mode.

tunnel mode { gre ip | ipip] }

Restore tunnel encapsulation mode.

no tunnel mode

Restore Default Configuration.

default tunnel mode

【Parameter Description】

Parameter	Description
gre ip	The transport network is an IPv4 network with GRE encapsulation.
ipip	The transport network is an IPv4 network without GRE encapsulation, and the user

	network is an IPv4 network. For manual tunnels, the peer IPv4 address needs to be configured.

【Default Configuration】gre ip

【Command Mode】 Interface mode

【Default Level】 2

【Usage Guide】 The encapsulation mode of Tunnel is the carrier protocol of Tunnel. The user can set the encapsulation mode of the tunnel interface according to the actual usage.

The actual tunnel mode type depends on the model used.

【Configuration Example]】1: Create a tunnel interface.

```
AC-FS(config)# interface tunnel 1
```

2: Set the tunnel mode.

```
AC-FS(config-if-Tunnel 1)# tunnel mode ipip
```

【Verification】1: Use the show interface tunnel command to view the tunnel mode.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

7.8 tunnel nested-limit

Sets the limit on the number of tunnel nesting encapsulation levels.

tunnel nested-limit number

Restore to default values.

no tunnel nested-limit

【Parameter Description】

Parameter	Description
number	The number of layers of tunnel nested encapsulation limit. The default is 4. The value range is 0～10.

【Default Configuration】4.

【Command Mode】 Interface mode

【Default Level】 2

【Usage Guide】 Tunnel nested encapsulation means that the packet is sent out after multiple layers of tunnel encapsulation in the local machine. Route changes on this machine can lead to infinite nested encapsulation of tunnels. Too many layers of nesting will result in continuous packet fragmentation and reassembly, which will seriously affect performance. In order to prevent the above phenomenon from happening, FS products have the function of automatically preventing infinite nested encapsulation. By default, only 4 levels of nesting are allowed. It can be modified by the tunnel nested-limit command.

It is very rare that nested encapsulation of tunnels is required, and it is usually a misconfiguration.

When Ruijie product finds that the number of tunnel encapsulation layers in the device may exceed the limit of nested encapsulation layers, it will automatically disable (down) the tunnel interface and print log information.

【Configuration Example]】1: Create a tunnel interface.

```
AC-FS(config)# interface tunnel 1
```

2: Set the tunnel mode.

```
AC-FS(config-if)# tunnel mode ipip
```

3: Set the limit on the number of tunnel nested encapsulation layers.

```
AC-FS(config-if)# tunnel nested-limit 5
```

【Verification】1: Use the show interface tunnel command to view the limit on the number of tunnel nested encapsulation layers.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

7.9 tunnel path-mtu-discovery

Activate the tunnel PMTUD (Path Maximum Transmission Unit Discovery) function.

tunnel path-mtu-discovery [age-timer { aging-mins | infinite } | min-mtu mtu-bytes]

Disable the tunnel PMTUD (Path Maximum Transmission Unit Discovery) function.

no tunnel path-mtu-discovery

【Parameter Description】

Parameter	Description
aging-mins	(Optional) Set the aging time of the MTU of the tunnel interface. After this time, the tunnel will send detection packets to find the path MTU; aging-mins: aging time, the range is 1-30 minutes, the default value is 10 minutes; infinite: forever Not aging.
mtu-bytes	(Optional) Set the MTU lower limit that the tunnel interface can be adjusted. The range is 92-65535 bytes, and the default value is 92 bytes.

【Default Configuration】 The PMTUD function is not enabled for the tunnel.

【Command Mode】 Interface mode

【Default Level】 2

【Usage Guide】 After the payload protocol packet is encapsulated by the tunnel, the packet size may exceed the MTU of the tunnel interface, resulting in packet fragmentation, even if the DF (Don't Fragment) bit is set in the payload protocol packet header. Ruijie products provide the tunnel path-mtu-discovery command in interface configuration mode, which can automatically detect the Path MTU of the peer end of the tunnel and dynamically adjust the mtu size of the tunnel interface to avoid packet fragmentation.

show interface tunnel may display the following states:

```
Path MTU Discovery state:init
Path MTU Discovery state:keep
Path MTU Discovery state:learning
```

Three state machines representing the learning process of PMTUD:

1. The initial configuration command is in the init state;

2. Send a probe message for learning, the status changes to learning, and a learning message is sent at this time;

3. When 5 probe packets are sent in a row and no MTU change is received, the state changes to keep and a keep packet is sent;

【Configuration Example]】1: Create a tunnel interface.

```
AC-FS(config)# interface tunnel 1
```

2: Set the tunnel mode.

```
AC-FS(config-if)# tunnel mode gre ip
```

3: Activate the PMTUD function of the tunnel and use the default Parameter.

```
AC-FS(config-if)# tunnel path-mtu-discovery
```

【Verification】 1: Use the show interface tunnel command to check whether PMTUD is enabled or disabled, and the specific Parameter.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

7.10tunnel protection ipsec profile

Configure the IPsec profile policy to protect the tunnel port.

tunnel protection ipsec profile WORD

Delete the IPSec profile policy of the tunnel interface.

no tunnel protection ipsec profile [WORD]

【Parameter Description】

Parameter	Description
Word	ipsec profile policy.

【Default Configuration】 The ipsec profile policy is not configured.

【Command Mode】 tunnel interface mode

【Default Level】 2

【Usage Guide】 You need to establish an ipsec profile first, and then associate the policy with the tunnel port.

【Configuration Example]】1: Create an ipsec profile policy.

```
AC-FS(config)#crypto ipsec profile test
```

2: Create a tunnel interface.

```
AC-FS(config)# interface tunnel 1
```

3: Associate the ipsec profile policy.

```
AC-FS(config-if)# tunnel protection ipsec profile test
```

【Verification】 1: Use the show interface tunnel command to view the ipsec policy configured for the tunnel.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

7.11 Tunnel source

Configure the source address of the tunnel interface.

tunnel source { ip-address | interface-type interface-number }

Delete the source address of the tunnel interface.

no tunnel source

【Parameter Description】

Parameter	Description
ip-address	Used to specify the local address of the tunnel.
interface-type	Common interface types, such as asynchronous serial interface Async, dial-up interface Dialer, Ethernet interface Ethernet, FastEthernet interface FastEthernet, Loopback interface, Null interface, and other Tunnel interfaces.
interface-number	interface number.

【Default Configuration】 The local address is not configured.

【Command Mode】 Interface mode

【Default Level】 2

【Usage Guide】 1. Each tunnel needs to configure the local address.

2. When specifying the local address as the address of an interface, select the primary IP address of this interface according to the tunnel mode.

3. Two automatic tunnels are not allowed to configure the same local address.

【Configuration Example]】1: Create a tunnel interface.

```
AC-FS(config)# interface tunnel 1
```

2: Set the tunnel mode.

```
AC-FS(config-if)# tunnel mode ipip
```

3: Configure the local address of the tunnel.

```
AC-FS(config-if)# tunnel source 1.1.1.1
```

【Verification】1: Use the show interface tunnel command to view the local address of the tunnel configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

7.12 tunnel tos

Configure the ToS byte of the outer transport protocol IPv4.

tunnel tos number

Unconfigure.

no tunnel tos

【Parameter Description】

Parameter	Description
number	The value of the ToS byte of the outer transport protocol IPv4. The value range is 0～255.

【Default Configuration】 If the tunnel inner layer bearer and outer layer encapsulation are both IPv4 protocol, the tos byte of the inner layer IPv4 header is copied to the outer layer IPv4 header by default. Otherwise, the outer IPv4 tos is 0.

【Command Mode】 Interface mode

【Default Level】 2

【Usage Guide】 If you want the priority of the tunnel packets to be higher, you can use the tunnel tos command to set it.

【Configuration Example]】1: Create a tunnel interface.

```
AC-FS(config)# interface tunnel 1
```

2: Set the tunnel mode.

```
AC-FS(config-if)# tunnel mode ipip
```

3: Configure the tunnel tos.

```
AC-FS(config-if)# tunnel tos 100
```

【Verification】 1: Use the show interface tunnel command to view the value of tunnel tos.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

7.13 tunnel ttl

Configure the ttl value of the tunnel interface.

tunnel ttl hop-count

Restore Default Configuration.

no tunnel ttl

【Parameter Description】

Parameter	Description
hop-count	Used to specify the ttl value of the tunnel interface. The range is 1~255, the default is 255.

【Default Configuration】 255.

【Command Mode】 Interface mode

【Default Level】 2

【Usage Guide】 Since the tunnel is a point-to-point link, for the load protocol, it looks like there is only one hop when routing, but in fact, the routing cost of the transport protocol may be more than one hop. FS products allow you to set the TTL of the tunnel, that is, to set the TTL value of the transport protocol header in the encapsulated packets sent by the tunnel. The tunnel intermediate node router decrements the TTL value in the transport protocol header and discards packets with a TTL of 0.

【Configuration Example]】 1: Create a tunnel interface.

```
AC-FS(config)# interface tunnel 1
```

2: Set the tunnel mode.

```
AC-FS(config-if)# tunnel mode ipip
```

3: Configure tunnel ttl.

```
AC-FS(config-if)# tunnel ttl 100
```

【Verification】 1: Use the show interface tunnel command to view the ttl value of the tunnel.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

7.14 Tunnel vrf

Configure the VPN where the transport network is located.

tunnel vrf vrf-name

Unconfigure.

no tunnel vrf

【Parameter Description】

Parameter	Description
vrf-name	The VPN where the transport network is located.

【Default Configuration】 The transmission network belongs to the global network, not in any VPN network.

【Command Mode】 Interface mode

【Default Level】 2

【Usage Guide】 Specify the VPN where the tunnel transmission network is located, that is, specify the VPN where the local address and the peer address are located, and the network between the local address and the peer address is also in this VPN.

【Configuration Example]】1: Create a tunnel interface.

```
AC-FS(config)# interface tunnel 1
```

2: Set the tunnel mode.

```
AC-FS(config-if)# tunnel mode ipip
```

3: Configure the VPN where the tunnel's transport network is located.

```
AC-FS(config-if)# tunnel vrf VPN1
```

【Verification】1: Use the show interface tunnel command to check whether the tunnel's transmission network is in the VPN, and which VPN it is in.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8 Network Connectivity Test Tools

8.1 clear rping table all

Clear all Rping entries.

clear rping table [all | [ping-object owner test-name] | [trace-object owner test-name]]

【Parameter Description】

Parameter	Description
owner	User index.
test-name	test index.

【Command Mode】 Privileged mode

【Default Level】-

【Usage Guide】 This command is used to delete all probe related entries of users managed by Rping on the device.

【Configuration Example】1: Clear all Rping entry information.

```
AC-FS# clear rping table all
```

2: Clear the concept line where the user is user and the probe name is AC-FS.

```
AC-FS# clear rping table user AC-FS
```

【Prompt Information】 1: If the concept line is not specified on the device, the corresponding information will be prompted.

【Platform Description】 -

8.2ping

Check whether the specified IPv4 address is reachable, and output relevant information.

ping [ip] [address [length length] [ntimes times] [timeout seconds] [data data] [source source] [df-bit] [validate] [detail]]

【Parameter Description】

Parameter	Description
address	pecify the destination IPv4 address or domain name.

length	Specify the length of the data padding segment of the sending packet, the range is 36~18024, and the default padding length is 100.
times	Specify the number of sent data packets, range: 1~ 4294967295.
seconds	Specify the timeout period, range: 1~10 (seconds).
data	Specifies the packet padding data, the format is a string with a length of 1-255, and the default padding is abcd.。
source	Specifies the source IPv4 address or source interface of the packet. Among them, loopback interface addresses (for example, 127.0.0.1) are not allowed as source addresses.
df-bit	Set the DF flag of IP. When the DF bit is set to 1, it means that the packet is not to be segmented. The default DF bit is 0.
validate	Set whether to verify the response message.
detail	Set whether to display detailed information in the echo. By default, it only displays '!'and'.'.

【Default Configuration】 By default, within the specified time (the default is 2 seconds), send 5 data packets with a length of 100 bytes to the specified IP address.

【Command Mode】 In normal user mode, only basic ping functions can be run; in privileged user mode, extended functions of ping can also be run.

【Default Level】 0

【Usage Guide】 Run the ping function, if there is a response, it will display the relevant information of the response, and finally output a statistical information. In the extended ping, you can specify the number, length, timeout, etc. of the sent data packets, which is the same as the basic ping function, and finally outputs a statistical information.
To use the domain name function, you need to configure the domain name server first. For details, please refer to the DNS configuration section.

【Configuration Example】1: An example of common ping. Specify the destination IP address as 192.168.21.26.

```
common ping
AC-FS# ping 192.168.21.26
Sending 5, 100-byte ICMP Echoes to 192.168.21.26, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

ping showing detail

```
AC-FS#ping 192.168.21.26 detail
Sending 5, 100-byte ICMP Echoes to 192.168.21.26, timeout is 2 seconds:
  < press Ctrl+C to break >
Reply from 192.168.21.26: bytes=100 time=4ms TTL=64
Reply from 192.168.21.26: bytes=100 time=3ms TTL=64
Reply from 192.168.21.26: bytes=100 time=1ms TTL=64
Reply from 192.168.21.26: bytes=100 time=1ms TTL=64
Reply from 192.168.21.26: bytes=100 time=1ms TTL=64
```

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms.2: Instance of extended ping. Specify the destination IP The address is 192.168.21.26, the length of the sent data packet is 1500, the number of sent data packets is 20, the timeout time is 3 seconds, and the packet filling data is ffff, and set the source IP address to 192.168.21.99.

```
common ping
AC-FS# ping 192.168.21.26 length 1500 ntimes 100 data ffff source 192.168.21.99 timeout 3
Sending 100, 1500-byte ICMP Echoes to 192.168.21.26, timeout is 3 seconds:
  < press Ctrl+C to break >
```

```
!!!
```

8.3 show rping detail

View Rping information.

show rping detail

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】 -

【Usage Guide】 Use this command to view the total number of objects managed in Rping on the device, the number of users and other information.

【Configuration Example]】1: View the details of Rping

```
AC-FS#show rping detail
Total owner number: 2
Total test number: 4
owner: user1
   test name: taget_1         storage type: volatile
   test name: taget_2         storage type: nonVolatile
owner: user2
   test name: taget_1         storage type: permanent
   test name: taget_2         storage type: readOnly
```

Field Description:

Field	Description
Total owner number	total number of users.
Total test number	Total number of tests.
owner	Username.
test name	test name.
storage type	Concept row storage type.

【Prompt Information】

【Platform Description】 -

8.4 traceroute

Displays the gateways that IPv4 packets pass through from source address to destination address.

traceroute [ip] [adress [probe number] [source source] [timeout seconds] [ttl minimum maximum]]

【Parameter Description】

Parameter	Description
address	Specify the destination IPv4 address or domain name.
number	Specifies the number of probes to send, range: 1~255.
source	Specifies the source IPv4 address or source interface of the packet. where loopback interface addresses (for example, 127.0.0.1) are not allowed as source addresses.
seconds	Specify the timeout period, range: 1~10 (seconds).
minimum maximum	Specify the minimum and maximum TTL value, range: 1~255.

【Default Configuration】 The default timeout is 3 seconds, the number of sent probes is 3, and the minimum and maximum TTLs are 1 and 255, respectively.

【Command Mode】 In normal user mode, only basic traceroute functions can be run; in privileged user mode, extended functions of traceroute can also be run.

【Default Level】 0

【Usage Guide】 The Traceroute command is mainly used to check the connectivity of the network, and when a network fault occurs, accurately locate the fault location. To use the domain name function, you need to configure the domain name server first. For details, please refer to the DNS configuration section.

【Configuration Example]】1: List the traceroute example with smooth network.

```
AC-FS# traceroute 61.154.22.36
< press Ctrl+C  to  break  >
Tracing the route to 61.154.22.36
1.....192.168.12.1      0 msec  0 msec  0 msec
2       192.168.9.2       4 msec  4 msec 4 msec
3       192.168.9.1       8 msec  8 msec  4 msec
4       192.168.0.10      4 msec  28 msec  12 msec
5       202.101.143.130     4 msec  16 msec  8 msec
6       202.101.143.154    12 msec  8 msec  24 msec
7       61.154.22.36      12 msec  8 msec  22 msec
```

From the above results, you can see which gateways (1-6), while giving the time it takes to reach the gateway.

2: List the traceroute examples that some gateways in the network are blocked.

```
AC-FS# traceroute 202.108.37.42
< press Ctrl+C to break >
Tracing the route to 202.108.37.42
1.....192.168.12.1      0 msec  0 msec  0 msec
2       192.168.9.2         0 msec  4 msec 4 msec
3       192.168.110.1      16 msec  12 msec  16 msec
4       *  *  *
```

```
5.....61.154.8.129       12 msec  28 msec  12 msec
6       61.154.8.17         8 msec  12 msec  16 msec
7       61.154.8.250       12 msec  12 msec  12 msec
8       218.85.157.222     12 msec  12 msec  12 msec
9       218.85.157.130     16 msec  16 msec  16 msec
10       218.85.157.77     16 msec  48 msec  16 msec
11       202.97.40.65      76 msec  24 msec  24 msec
12       202.97.37.65      32 msec  24 msec  24 msec
13       202.97.38.162     52 msec  52 msec  224 msec
14       202.96.12.38       84 msec  52 msec  52 msec
15       202.106.192.226     88 msec  52 msec  52 msec
16       202.106.192.174     52 msec  52 msec  88 msec
17       210.74.176.158     100 msec  52 msec  84 msec
18       202.108.37.42      48 msec  48 msec  52 msec
```

From the above results, you can see which gateways (1-17), and gateway 4 fails.

3: List examples of using the domain name function.

```
AC-FS# traceroute www.ietf.org
Translating " www.ietf.org "...[OK]
< press Ctrl+C  to  break  >
Tracing the route to 64.170.98.32
1.....192.168.217.1    0 msec  0 msec  0 msec
2       10.10.25.1          0 msec  0 msec  0 msec
3       10.10.24.1          0 msec  0 msec  0 msec
4       10.10.30.1          10 msec 0 msec  0 msec
5       218.5.3.254         0 msec  0 msec  0 msec
6       61.154.8.49         10 msec 0 msec  0 msec
7       202.109.204.210     0 msec  0 msec  0 msec
8       202.97.41.69        20 msec 10 msec 20 msec
9       202.97.34.65        40 msec 40 msec 50 msec
10      202.97.57.222       50 msec 40 msec 40 msec
11      219.141.130.122     40 msec 50 msec 40 msec
12      219.142.11.10       40 msec 50 msec 30 msec
13      211.157.37.14       50 msec 40 msec 50 msec
14      222.35.65.1         40 msec 50 msec 40 msec
15      222.35.65.18        40 msec 40 msec 40 msec
16      222.35.15.109       50 msec 50 msec 50 msec
17      *       *       *
18     64.170.98.32        40 msec 40 msec 40 msec
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

9 TCP

9.1ip tcp adjust-mss

Set the MSS option value of forwarded TCPv4 SYN packets.

ip tcp adjust-mss max-segment-size

Restore Default Configuration.

no ip tcp adjust-mss

【Parameter Description】

Parameter	Description
max-segment-size	Maximum data segment size, in bytes, range is 500-1460.

【Default Configuration】 Do not modify the MSS option value of the SYN packet.

【Command Mode】 Interface mode

【Default Level】 14

【Usage Guide】 MSS: The maximum value of the data payload of a TCP packet.

The path MTU discovery function of TCP is implemented according to RFC1191, and this function can improve the utilization rate of network bandwidth. When users use TCP to transmit large blocks of data in batches, this feature can significantly improve transmission performance.

When the client initiates a tcp connection, it negotiates the maximum value of the data payload of the TCP message through the MSS option Field in the TCP SYN message. The MSS value of the client SYN message indicates the maximum data payload of the subsequent TCP message sent by the server. value, and vice versa.

Configuring this command on an interface will change the MSS option of the SYN packet received or sent by the interface to the MSS value configured on the interface. If both the ingress and egress of SYN packets are configured with MSS, the smaller of the two ports is used. However, it is generally recommended that the egress and ingress configurations be the same. This command actually modifies the SYN message exchanged when TCP establishes a connection, and some versions also modifies the SYN+ACK message.

Enabling and disabling this function does not take effect for the established TCP connection, but only for the later established TCP connection.

【Configuration Example]】 1: Configure on interface GigabitEthernet 0/0 to modify the MSS option value of the forwarded TCPv4 SYN packet to 1000 bytes.

```
AC-FS(config-if-GigabitEthernet 0/0)# ip tcp adjust-mss 1000
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

9.2 ip tcp keepalive

This command is used to enable the TCP keep-alive function.

ip tcp keepalive [interval num1] [times num2] [idle-period num3]

【Parameter Description】

Parameter	Description
interval num1	The interval for sending keep-alive packets, in seconds, ranging from 1 to 120. The default value is 75 seconds.
times num2	The number of times to send keep-alive packets, the range is 1 to 10, and the default value is 6.
idle-period num3	Idle time, that is, the length of time that the peer end has not sent packets to the local end, in seconds, the value range is 60 to 1800, and the default value is 15 minutes.

【Default Configuration】 Close.

【Command Mode】 Global mode

【Default Level】 2

【Usage Guide】 If TCP wants to know whether the peer is still working normally, you can enable the keep-alive function. Assuming that the user enables the keep-alive function, the time interval, number of times and idle time are all defaulted. TCP has not received any packets sent by the peer within 15 minutes, and starts to send keep-alive packets, which are sent every 75 seconds. Send 6 times in a row, if no TCP message sent by the other party is received, the TCP connection is considered invalid and the TCP connection is automatically released.

This command no longer distinguishes between server and client, and is valid for all TCP connections.

【Configuration Example]】1: Enable the TCP keep-alive function on the device, the idle time is 3 minutes, and the interval for sending keep-alive packets is 60 seconds. If a TCP message is sent, the TCP connection is considered invalid.

```
AC-FS(config)# ip tcp keepalive interval 60 times 4 idle-period 180
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 This command was introduced in version 11.0, replacing the configuration commands "service tcp-keepalives-in" and "service tcp-keepalives-out" in version 10.x.

9.3 ip tcp mss

Sets the maximum value of MSS for TCP connections.

ip tcp mss max-segment-size

Restore Default Configuration.

no ip tcp mss

【Parameter Description】

Parameter	Description
max-segment-size	Upper limit of MSS. The unit is byte, the value range is 68-10000. By default, MSS calculated from MTU is used.

【Default Configuration】-

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 The function of ip tcp mss is to limit the maximum value of the MSS of the upcoming TCP connection. The negotiated MSS value for any newly established connection cannot exceed the configured value. If you want to reduce the maximum MSS value of the connection, you can configure this command, but in general, no configuration is required. By default, the MSS calculated from the MTU is used, as follows:

IPv4 TCP: MSS = IP MTU of the egress corresponding to the peer IP address - 20-byte IP header - 20-byte TCP header.

If the connection supports certain options, the MSS is also subtracted from the 4-byte aligned length of the option. For example, the MD5 option needs to subtract 20 bytes, the MD5 option length is 18 bytes, and the alignment is 20 bytes.

If the MSS is configured by the user, the actual effective MSS is the smaller value of the MSS calculated according to the MTU and the MSS configured by the user.

【Configuration Example]】1: Set the upper limit of the MSS of the TCP connection to 1300 bytes.

```
AC-FS(config)# ip tcp mss 1300
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 This command is only valid for IPv4 TCP.

9.4 ip tcp path-mtu-discovery

Enables path MTU discovery for TCP.

ip tcp path-mtu-discovery [age-timer minutes | age-timer infinite]

Disable the TCP path MTU discovery function.

no ip tcp path-mtu-discovery

【Parameter Description】

Parameter	Description
age-timer minutes	The interval at which TCP re-probes after discovering the PMTU. The unit is minute, the value range is 10-30. The default value is 10.
age-timer infinite	TCP does not re-probe after discovering PTMU.

【Default Configuration】 Close.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 The path MTU discovery function of CP is implemented according to RFC1191, and this function can improve the utilization rate of network bandwidth. When users use TCP to transmit large blocks of data in batches, this feature can significantly improve transmission performance.

According to the Description of RFC1191, after TCP discovers PMTU, it can use larger MSS to detect new PMTU at intervals. This time interval is specified using the Parameter age-timer. When the PMTU discovered by the device is smaller than the MSS negotiated by both ends of the TCP connection, the device will try to discover a larger PMTU according to the above configured time interval. The probing process will not stop until the PMTU reaches the MSS value, or the user stops the timer. To stop this timer, use age-timer infinite Parameter.

【Configuration Example】1: Enable PMTU discovery function.

```
AC-FS(config)# ip tcp path-mtu-discovery
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 This command is valid for IPv4 TCP.

9.5 ip tcp send-reset

Allows to send reset packets when receiving TCP packets with unreachable ports.

ip tcp send-reset

It is forbidden to send reset packets when receiving TCP packets whose ports are unreachable.

no ip tcp send-reset

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 Send a reset message when receiving a TCP message whose port is unreachable.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Under normal circumstances, when the TCP module distributes a TCP message, if it cannot find the TCP connection to which the message belongs, it will actively reply a reset message to terminate the TCP connection of the opposite end. However, this will also become an attack target of attackers. A large number of TCP packets with unreachable ports will cause attacks on the device. You can use the following commands to prohibit sending reset packets to packets with unreachable ports.

【Configuration Example]】1: Disable sending reset packets when receiving TCP packets whose ports are unreachable.

```
AC-FS(config)# no ip tcp send-reset
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 Version 11.0 discards the configuration command "ip tcp not-send-rst" of version 10.x, and is compatible with version 10.x. If the configuration command of version 10.x is executed, it will be automatically converted to version 11.0. configuration command.

This command takes effect only for IPv4 TCP.

9.6 ip tcp synwait-time

Set the timeout period of SYN packets for establishing connections.

ip tcp synwait-time seconds

Restore default values.

no ip tcp synwait-time

【Parameter Description】

Parameter	Description
seconds	SYN message timeout time. The unit is seconds, the value range is 5-300, and the default value is 20.

【Default Configuration】 The default timeout is 20 seconds.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】If there is a SYN attack in the network, reducing the SYN timeout time can prevent some resource consumption, but it will not be effective for continuous SYN attacks. When the device actively establishes a connection with the external request, reducing the SYN timeout time can reduce the user waiting time, such as telnet. If the network is poor, the timeout period can be appropriately increased.

【Configuration Example】1: Set the timeout period of the SYN message for establishing a connection to 10 seconds.

```
AC-FS(config)# ip tcp synwait-time 10
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 Version 11.0 discards the configuration command "ip tcp synctime-out" of version 10.x, and is compatible with version 10.x. If the configuration command of version 10.x is executed, it will be automatically converted to the configuration command of version 11.0 .

In version 10.x, this command is only valid for IPv4 TCP.

9.7ip tcp window-size

Set the TCP window size.

ip tcp window-size size

Restore default values.

no ip tcp window-size

【Parameter Description】

Parameter	Description
size	window size. The unit is byte, the value range is 128-(65535 << 14), and the default value is 65535.

【Default Configuration】 The default value is 65535 bytes.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】The TCP receive buffer is used to buffer the data received from the peer, which will be read by the application later. In general, TCP's window value reflects the size of the free space in the receive buffer. For connections with large bandwidth and large batches of data, increasing the window can significantly improve TCP transmission performance.
If the window is larger than 65535 bytes, the window expansion function is automatically enabled.

【Configuration Example]】1: Set the window size to 16386 bytes.

```
AC-FS(config)# ip tcp window-size 16386
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 This command is only valid for IPv4 TCP.

9.8 service tcp-keepalives-in

Enable the keep-alive function on the TCP server side.

service tcp-keepalives-in [interval] [garbage]

Disable the keep-alive function on the TCP server side

no service tcp-keepalives-in

【Parameter Description】

Parameter	Description
interval	The interval for sending keep-alive packets, in seconds, the value range is 1 to 65535, the default value is 60 seconds.
garbage	Keep-alive packets carry one byte of invalid data, which is not carried by default.

【Default Configuration】 Disable the keep-alive function of the TCP server

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Sometimes the TCP server wants to know whether the client is still working normally, which requires the use of the TCP keep-alive function.

If the keep-alive message is sent 4 times in a row and no TCP message is received from the other party, the TCP connection is considered invalid and the TCP connection is automatically released.

【Configuration Example]】1: Enable the keep-alive function on the TCP server side, the interval for sending keep-alive packets is 10 seconds, and the keep-alive packets carry one byte of invalid data.

```
AC-FS(config)# service tcp-keepalives-in 10 garbage
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 This command is discarded in version 11.0. This command is hidden. If the user executes this command, it will be converted into a new configuration command "ip tcp keepalive" and saved.

9.9 service tcp-keepalives-out

Enable the keep-alive function of the TCP client.

service tcp-keepalives-out [interval] [garbage]

【Parameter Description】

Parameter	Description
interval	The interval for sending keep-alive packets, in seconds, the value range is 1 to 65535, the default value is 60 seconds.
garbage	Keep-alive packets carry one byte of invalid data, which is not carried by default.

【Default Configuration】 Disable the keep-alive function of the TCP client.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 The TCP client can use the keep-alive function to detect whether the server is still working normally.
If the keep-alive message is sent 4 times in a row and no TCP message is received from the other party, the TCP connection is considered invalid and the TCP connection is automatically released.

【Configuration Example]】1: Enable the keep-alive function of the TCP client, the interval for sending keep-alive packets is 10 seconds, and the keep-alive packets carry one byte of invalid data.

```
AC-FS(config)# service tcp-keepalives-out 10 garbage
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 This command is discarded in version 11.0. This command is hidden. If the user executes this command, it will be converted into a new configuration command "ip tcp keepalive" and saved.

9.10 show tcp connect

Displays basic information about the system's current IPv4 TCP connections.

show tcp connect [local-ip a.b.c.d] [local-port num] [peer-ip a.b.c.d] [peer-port num]

Displays statistics about the system's current IPv4 TCP connections.

show tcp connect statistics

【Parameter Description】

Parameter	Description
local-ip a.b.c.d	local IP address.
local-port num	local port.
peer-ip a.b.c.d	Peer IP address.
peer-port num	peer port.

statistics	View statistics for IPv4 TCP connections.

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】 -

【Configuration Example】 1: View the basic information of the current IPv4 TCP connection of the system.

```
AC-FS#show tcp connect
Number Local Address      Foreign Address          State       Process  name
1      0.0.0.0:22.....0.0.0.0:0                    LISTEN      rg-sshd
2      0.0.0.0:23         0.0.0.0:0                LISTEN      rg-telnetd
3      1.1.1.1:23         1.1.1.2:64201            ESTABLISHED rg-telnetd
```

Field Description:

Field	Description
Number	serial number.
Local Address	Local address and port number. The number after the colon is the port number. For example, "23" in "1.1.1.1:23" is the port number.
Foreign Address	The remote address and port number. The number after the colon is the port number. For example, "23" in "1.1.1.1:23" is the port number.
State	The current state of the TCP connection, there are 11 possible states: CLOSED: Connection disconnected LISTEN: Listening state. SYNSENT: SYN message has been sent, three-way handshake stage SYNRCVD: SYN message has been received, three-way handshake stage ESTABLISHED: connection has been established FINWAIT1: The local end has sent a FIN message FINWAIT2: The FIN message sent by the local end has been confirmed CLOSEWAIT : The local end has received the FIN message from the peer end. LASTACK: The local end receives the FIN message from the peer end, and then the local end sends its own FIN message. CLOSING: The local end sends a FIN message and receives the FIN message from the peer end before the peer end responds with the ACK message of the FIN message. message TIMEWAIT: The FIN message sent by the local end has been confirmed, and the local end has also confirmed the received FIN message.

Process name	process name.

2: View the statistics of the current IPv4 TCP connections of the system.

【Prompt Information】 -

【Platform Description】 -

9.11 show tcp parameter

Display the current TCP Parameter information of the system.

show tcp parameter

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】 -

【Configuration Example]】 1: View the current tcp Parameter information of the system

```
AC-FS#show tcp parameter
Hash table information:
  Established hash bucket size: 16384
  Bind hash bucket size: 16384
Memory information:
  Global memory limit: low=92160, pressure=122880, high=184320 (unit: pages)
  Per-socket receive buffer size: min=4096, default=87380, max=3932160 (unit: bytes)
  Per-socket send buffer size: min=4096, default=16384, max=3932160 (unit: bytes)
  Current allocated memory: 0
  Current memory pressure flag: 0
SYN specific information:
  Max SYN_RECV sockets per LISTEN socket: 65535
  Max SYN retries: 5
  Max SYN ACK retries: 5
Timewait specific information:
  Max timewait sockets: 180000
  Current timewait sockets: 0
  Timewait recycle: 0
  Reuse timewait port: 0
Keepalive information:
  Keepalive on: 0
  Idle period: 900 seconds
```

```
  Interval: 75 seconds
  Max probes: 6
MTU probing:
  Enable mtu probing: 0
FIN specific information:
  FIN_WAIT_2 timeout: 60 seconds
Orphan socket information:
  Max orphans: 16384
  Max orphan retries: 0
  Current orphans: 0
```

Field Description:

Field	Description
Hash table information	TCP connection hash table Parameter information.
Memory information	TCP connection send and receive buffer Parameter information.
SYN specific information	TCP server connection listening related Parameter information.
Timewait specific information	TCP connection parameter information in TIMEWAIT state.
Keepalive information	TCP keep-alive clock Parameter information.
MTU probing	Parameter information related to MTU detection.
FIN specific information	Parameter information about TCP connection close.
Orphan socket information	Parameter information for TCP connections not associated with specific applications.

【Prompt Information】-

9.12 show tcp pmtu

Displays the path MTU for IPv4 TCP connections.

show tcp pmtu [local-ip a.b.c.d] [local-port num] [peer-ip a.b.c.d] [peer-port num]

【Parameter Description】

Parameter	Description
local-ip a.b.c.d	local IP address.
local-port num	local port.
peer-ip a.b.c.d	Peer IP address.
peer-port num	peer port.

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】-

【Configuration Example]】 1: View the path MTU of the IPv4 TCP connection.

```
AC-FS# show tcp pmtu
Number  Local Address           Foreign Address        PMTU
1       192.168.195.212.23   192.168.195.112.13560   1440
```

Field Description:

Field	Description
Number	serial number.
Local Address	Local address and port number, the number after the colon is the port number, such as "23" in "192.168.195.212.23" is the port number.
Foreign Address	The remote address and port number, the number after the colon is the port number, such as "23" in "192.168.195.212.23" is the port number.
PMTU	Path MTU.

【Prompt Information】-

【Platform Description】 -

9.13 show tcp port

Displays the current TCP port usage of the system.

show tcp port [num]

【Parameter Description】

Parameter	Description
num	The port number.

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】-

【Configuration Example]】1: View the current usage of the system's IPv4 TCP port.

```
AC-FS#show tcp port
TCP connections on port 23:
Number  Local Address Foreign Address    State
```

```
1       1.1.1.1:23.....1.1.1.2:64571    ESTABLISHED
Total: 1

TCP connections on port 2650:
Number Local Address Foreign Address State
Total: 0
```

Field Description:

Field	Description
Number	serial number
Local Address	Local address and port number.
Foreign Address	Remote address and port number.
State	The current state of the TCP connection, there are 11 possible states: CLOSED: The connection has been disconnected. LISTEN: listening status. SYNSENT: SYN message has been sent, three-way handshake stage SYNRCVD: SYN message has been received, three-way handshake stage ESTABLISHED: connection has been established FINWAIT1: The local end has sent a FIN message FINWAIT2: The FIN message sent by the local end has been confirmed CLOSEWAIT : The local end has received the FIN message from the peer end. LASTACK: The local end receives the FIN message from the peer, and then the local end sends its own FIN message. CLOSING: The local end sends a FIN message and receives the FIN message from the peer end before the peer end responds with an ACK message for the FIN message.. TIMEWAIT: The FIN message sent by the local end has been confirmed, and the local end has also confirmed the received FIN message.

【Prompt Information】-

【Platform Description】 -

9.14 show tcp statistics

Display the current TCP statistics of the system, including message reception information, three-way handshake information, and time-wait connection information.

show tcp statistics

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】-

【Configuration Example]】 1: View the current tcp statistics of the system:

```
AC-FS#show tcp statistics
TCP Packets
  Received: 1103
  Errors : 0(checksum: 0)
Three way handshake
  Request queue overflow: 0
  Accept backlog full: 0
  Web authentication limit per user: 0
  Failed to alloc memory for request sock: 0
  Failed to create open request child: 0
  SYN ACK retransmits: 0
  Timeouted requests: 0
Time-wait
  Time-wait bucket table overflow: 0
```

Field Description:

Field	Description
TCP Packets	Normal packets received by TCP, error packets.
Three way handshake	Information in the three-way handshake process, including the number of connection requests received, as the number of connections between the server and the client, the number of times the three-way handshake failed due to WEB authentication restrictions, the number of times the TCP socket could not be created due to insufficient memory, and the number of times the TCP socket could not be created. The number of sub-connections created, the number of packet

	retransmissions, and the number of times the connection was not established due to the packet retransmission timeout.
Time-wait	TIMEWAIT state connection information.

【Prompt Information】-

10 Software IPv4 Fast Forwarding

10.1 clear ip ref packet statistics

Clears the current packet statistics of IPv4 fast forwarding.

clear ip ref packet statistics

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Clear the current packet statistics of IPv4 fast forwarding.

```
AC-FS #clear ip ref packet statistics
```

【Prompt Information】-

【Platform Description】 -

10.2ip ref load-sharing original

Configure the load balancing algorithm for IPv4 fast forwarding to load balancing based on the destination IP address and source IP address.

ip ref load-sharing original

Restore the load balancing algorithm of IPv4 fast forwarding to the default value.

no ip ref load-sharing original

【Parameter Description】

Parameter	Description

-	-

【Default Configuration】 Load balancing based on destination IP address

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Software Fast Forwarding is responsible for data forwarding and supports two load balancing algorithms, one is destination IP load balancing, and the other is a load balancing algorithm combining destination IP and source IP. When forwarding IP packets through multiple paths, if the current setting is destination IP load balancing, REF will forward the packets by matching one of the paths with the destination IP of the packet. The default is destination IP load balancing.

【Configuration Example]】1: Configure the balanced routing algorithm of source IP+destination IP.

```
AC-FS(config)# ip ref load-sharing original
```

2: Use the balanced routing algorithm based on the destination address of the packet.

```
AC-FS(config)# no ip ref load-sharing original
```

【Verification】Use the command show run to view the configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

10.3 show ip ref adjacency

Display the information of a specific adjacent node or all current adjacent nodes.

show ip ref adjacency [glean | local | ip-address | interface interface_type interface_number | discard | statistics]

【Parameter Description】

Parameter	Description

glean	collection of adjacent nodes.
local	local neighbor.
ip-address	Adjacent next hop IP.
interface_type	Specify the interface type.
interface_number	Specify the interface number.
discard	show dropped neighbors.
statistics	Statistics.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 This command can display the adjacency table information of the current IPv4 fast forwarding. It can be specified to display aggregate adjacency, local adjacency, adjacency corresponding to a specified IP, adjacency associated with a specified interface, and related information of all adjacent nodes.

【Configuration Example]】 1: Display all adjacency information in the adjacency table.

```
AC-FS#show ip ref adjacency
id state      type    rfct chg  ip            interface         linklayer(header data)
1  unresolved mcast   1    0.....224.0.0.0
9  resolved   forward 1    0    192.168.50.78   GigabitEthernet 0/0  00 25 64 C5 9D 6A 00 D0 F8 98
76 54 08 00
7  resolved   forward 1    0    192.168.50.200  GigabitEthernet 0/0  00 04 5F 87 69 66 00 D0 F8 98
76 54 08 00
6  unresolved  glean  1    0    0.0.0.0         GigabitEthernet                              0/0
4  unresolved  local  3    0    0.0.0.0         Local 1
```

Field Description of the displayed results:

Field	Description
id	Adjacency ID.
state	Adjacency. unresolve: not resolved. resolved: resolved.

type	Adjacency type. local: local adjacency. forward: forwarding adjacency. discard: discard the adjacency. glean: set adjacency. mcast: multicast adjacency.
rfct	adjacency referenced count.
chg	Whether the adjacency is in the change chain.
ip	The IP address corresponding to the adjacency.
interface	Outgoing interface.
linklayer	second layer header.

【Prompt Information】-

【Platform Description】 -

10.4 show ip ref exact-route

Displays the exact forwarding path of IP packets.

show ip ref exact-route source_ipaddress dest_ipaddress

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 With this command, you can specify the source IP address and destination IP address of IP packets to display the forwarding path of specific packets.

【Configuration Example]】1: View the forwarding path from 192.168.217.74 to 192.168.13.1.

```
AC-FS# show ip ref exact-route 192.168.217.74 192.168.13.1
192.168.217.74------> 192.168.13.1 (vrf index: 0):
id state    type    rfct chg  ip            interface          linklayer(header data)
9  resolved forward 1     0   192.168.17.1  GigabitEthernet 0/0 00 25 64 C5 9D 6A 00 D0 F8 98 76
54 08 00
```

Field Description of the displayed results:

Field	Description
id	Adjacency ID.
state	Adjacency. unresolve: not resolved. resolved: resolved.
type	Adjacency type. local: local adjacency. forward: forwarding adjacency. discard: discard the adjacency. glean: set adjacency. mcast: multicast adjacency.
rfct	adjacency referenced count.
chg	Whether the adjacency is in the change chain.
ip	The IP address corresponding to the adjacency.
interface	Outgoing interface.
linklayer	second layer header.

【Prompt Information】 -

【Platform Description】 -

10.5 show ip ref packet statistics

Displays the current packet statistics of IPv4 fast forwarding.

show ip ref packet statistics

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Display the current packet statistics of IPv4 fast forwarding.

```
AC-FS #show ip ref packet statistic
ref packet statistic:
     bad head        : 0
     lookup fib fail : 0
     local adj       : 0
     glean adj       : 0
     forward         : 0
     redirect        : 0
     ttl expiration  : 0
     no ip routing   : 0
```

Field Description of the displayed results:

Field	Description
bad head	Number of packets with header errors.
lookup fib fail	Number of fast forwarding route selection failed packets.
local adj	Number of packets matching the local adjacency.
glean adj	Number of packets matched to the aggregation adjacency.
for ar	Number of packets matched to forwarding adjacencies.
redirect	Number of packets processed by redirection.
ttl expiration	Number of packets whose packet TTL times out.
no ip routing	The number of packets that are not allowed to be forwarded locally.

【Prompt Information】-

【Platform Description】 -

10.6 show ip ref resolve-list

Displays IPv4 fast-forward active resolution information.

show ip ref resolve-list

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Display IPv4 fast forwarding active resolution information.

```
AC-FS#show ip ref resolve-list
IP                res_state flags interface
1.1.1.1           unres     1      GigabitEthernet 0/0
```

Field Description:

Field	Description
IP	IP address.
res_state	unres: unresolved, res: resolved.
flags	0: not related to adjacency, 1: related to adjacency.
interfa e	interface name.

【Prompt Information】-

【Platform Description】 -

10.7 show ip ref route

Displays all routing information for the current IPv4 fast forwarding.

show ip ref route [default | ip mask | statistics]

【Parameter Description】

Parameter	Description
default	Specify default route.
ip	Specify the routing destination IP.
mask	Specify routing mask.

statistics	Statistics.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 It can display the routing information of the current IPv4 fast forwarding, and can specify to display the default route, the route matching the specified IP/MASK, and all the routing information.

【Configuration Example]】 1: Display all routing information in the global fast forwarding table.

```
AC-FS#show ip ref route
Codes: * - default route
       # - zero route
 ip/mask            weight  path-id      next-hop        interface
 255.255.255.255/32 1       4.....0.0.0.0          Local 1
 224.0.0.0/24       1       4            0.0.0.0         Local 1
 192.168.50.0/24    1       6            0.0.0.0         GigabitEthernet 0/0
 192.168.50.200/32  1       7            192.168.50.200  GigabitEthernet 0/0
 192.168.50.122/32  1       4            0.0.0.0         Local 1
 192.168.50.78/32   1       9            192.168.50.78   GigabitEthernet 0/0
```

Field Description of the displayed results:

Field	Description
ip/mask	Destination IP address and mask length.
path-id	Adjacency Index ID.
weight	routing weight.
next_hop	Next hop.
interface	Output Interface.

【Prompt Information】 -

【Platform Description】 -

11 TFTP-Server

11.1 tftp-server enable

Start the TFTP server.

tftp-server enable

Stop the TFTP server.

no tftp-server enable

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 Closed state

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 When the TFTP server is enabled, the TFTP client can connect to it and perform file upload or download operations. This command and the tftp-server topdir command must be configured to enable the TFTP client to access files on the TFTP server. .

【Configuration Example]】1: Start the TFTP server and restrict the client to access only the syslog subdirectory.

```
AC-FS(config)# tftp-server topdir /syslog
AC-FS(config)# tftp-server enable
```

2: Shut down the TFTP server.

```
AC-FS(config)# no tftp-server enable
```

【Verification】1:show run You can see that the configuration is successful.

【Common Mistake】-

【Platform Description】 -

11.2 tftp-server topdir

Restricts the directory range that TFTP clients can read and write files to.

tftp-server topdir directory

Use the no form of this command to completely prohibit the client from accessing any files on the TFTP server.

no tftp-server topdir

Restore Default Configuration.

default tftp-server topdir

【Parameter Description】

Parameter	Description
directory	The top-level directory that the TFTP client can operate on, "/" represents the root directory.

【Default Configuration】 There is no top-level directory setting by default (no reading and writing of any directory is allowed)

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 The top-level directory of the TFTP server limits the range of file directories that the client can access after logging in.

The top-level directory must be specified correctly for TFTP clients to access files on the TFTP server.

If this command is not configured, the TFTP client will not be able to access any files or directories on the server.

【Configuration Example]】1: Start the TFTP server and restrict the client to access only the syslog subdirectory.

```
AC-FS(config)# tftp-server topdir /syslog
AC-FS(config)# tftp-server enable
```

2: Cancel the configuration of the root directory.

```
AC-FS(config)# no tftp-server topdir
```

【Verification】1: show run can see that the configuration is successful

【Prompt Information】 1: Configure a directory that does not exist.

```
% topdir /ab don't exist!
```

2: Configure an illegal directory.

% Root dir too long, max length is 64.

【Common Mistake】 18. Configure a directory that does not exist.

19. Configure illegal directory.

【Platform Description】 -

11.3 show tftp-server

Display the current tftp server configuration

show tftp-server

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged user mode, global configuration mode, interface configuration mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example]】1: View the download progress of the TFTP client.

```
AC-FS# show tftp-server
    tftp-server information
==================================
enable  :  Y
topdir : flash:/
```

Field Description:

Field	Description
enable	Whether the TFTP server is started.
topdir	Top-level directory for TFTP server configuration.

【Prompt Information】-

【Platform Description】 -

11.4 show tftp-server updating-list

Display the download progress of the current tftp client

show tftp-server updating-list

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged user mode, global configuration mode, interface configuration mode

【Default Level】 14

【Usage Guide】Only supported on AM5528 products

【Configuration Example]】 1: View the download progress of the TFTP client.

```
AC-FS# show  tftp-server updating-list
IP Address              Interface                File Name                TX          Elapsed
----------------------  -----------------------  -----------------------  ----------  --------
171.208.208.2           GigabitEthernet 0/7      main_map552.bin           6.28392%   00:00:05
```

Field Description:

Field	Description
IP Address	IP address of the TFTP client.
Interface	The name of the Layer 2 interface used for downloading by the TFTP client.
File Name	Filename requested by the TFTP client.
TX	The current download progress of the TFTP client (value as a percentage).
Elapsed	TFTP client download elapsed time.

【Prompt Information】-

【Platform Description】 -

12 NAT

12.1 address

Configure an address range for a NAT empty address pool

address start-ip end-ip [match interface interface]

Delete an address pool address range

no address start-ip end-ip [match interface interface]

Configure an address range for a NAT empty address pool

address interface interface [match interface interface]

Delete an address pool address range

no address interface interface [match interface interface]

【Parameter Description】

Parameter	Description
start-ip	The starting IP address of an address block.
end-ip	The ending IP address of an address block.
interface interface	It is used when NAT has multiple outside ports. The address defined in the Pool adopts the interface address, which is generally used when the interface address needs to be negotiated and is unknown at the beginning. Note that it should be used in conjunction with the following match interface interface, and the two interfaces should be consistent. Otherwise, NAT may fail.
match interface interface	It is used when NAT has multiple outside ports. When the route determines the packet's exit, NAT uses this exit to select the matching address in the pool.

【Default Configuration】 No address range is defined.

【Command Mode】 NAT address pool configuration mode

【Default Level】 14

【Usage Guide】 If an address pool needs to define multiple address ranges, you need to enter the NAT address pool configuration mode first, and then define the NAT address range. This command does not support configuration using AP member ports

【Configuration Example]】 1: Create a mulnets address pool and define two address blocks.

```
AC-FS(config)# ip nat pool mulnets netmask 255.255.255.0
AC-FS(config-nat)# address 172.16.10.1 172.16.10.254
AC-FS(config-nat)# address 192.168.100.1 192.168.100.50
```

【Prompt Information】 1: If the end IP address configured by this command is smaller than the start IP address, the configuration fails, and prompts:

```
% End address less than start address
```

2: If the start IP address and end IP address configured by this command are not in the same network segment, the configuration fails, and prompts:

```
% Start and end addresses on different subnets
```

3: If the start IP address and end IP address configured by this command are both 0.0.0.0, the configuration fails, prompting:

```
% Ip address 0.0.0.0 ~ 0.0.0.0 are invalid.
```

4: If the command uses the AP member port for configuration, the configuration fails, prompting:

```
% Not permit ap member interface.
```

5: If the number of address ranges in an address pool exceeds 100, the configuration fails, prompting:

```
% Reach max pool addr range
```

6: If the memory is insufficient when configuring this command, the configuration fails, prompting:

```
% Create address range fail
```

7: If the configured address range uses the interface address and already exists, the configuration fails, and prompts:

```
% already use this interface's ip address,please delete and recreate
```

8: If the configured address range already exists, the configuration fails, prompting:

```
% Already exist this range,please delete and recreate
```

9: If the configured address range uses the interface address and overlaps with the existing address, the configuration fails and prompts:

```
% Use interface's ip address overlap with existing range
```

10: If the configured address range conflicts with the existing address, the configuration fails, prompting:

```
%Start and end addresses overlap with existing range
```

11: If the address range with an interface is deleted and does not exist, the configuration fails, and the prompt:

```
% address range with interface not exist
```

12: If the deleted address range does not exist, the configuration fails, prompting:

```
% Address range x.x.x.x-x.x.x.x not exist
```

【Common Mistake】-

【Platform Description】 -

12.2ip nat

To NAT the data traffic sent and received on an interface.

ip nat { inside | outside }

Make an interface no longer apply NAT.

no ip nat { inside | outside }

【Parameter Description】

Parameter	Description
inside	Indicates that the interface is connected to the internal network.
outside	Indicates that the interface is connected to an external network.

【Default Configuration】 When the interface sends and receives data, NAT is not applied.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】NAT translation will be performed only when the data packets are routed between the outside interface and the inside interface and meet certain rules. therefore support

A NAT device must be configured with at least one inside interface and one outside interface.

【Configuration Example]】1: The following configuration example can dynamically convert the 192.168.12.0/24 internal host to the global address 200.168.12.0/28 network segment. Hosts on other network segments of the internal network are not allowed to do NAT.

```
AC-FS#configure terminal
AC-FS(config)# interface GigabitEthernet 0/0
AC-FS(config-if-GigabitEthernet 0/0)# ip address 192.168.12.6 255.255.255.0
AC-FS(config-if-GigabitEthernet 0/0)# ip nat inside
AC-FS(config-if-GigabitEthernet 0/0)# exit AC-
FS(config)# interface GigabitEthernet 0/1
AC-FS(config-if-GigabitEthernet 0/1)# ip address 200.168.12.17 255.255.255.0
AC-FS(config-if-GigabitEthernet 0/1)# ip nat outside
AC-FS(config-if-GigabitEthernet 0/1)# exit
AC-FS(config)# ip nat pool net200 200.168.12.1 200.168.12.15 netmask 255.255.255.0 AC-
FS(config)# ip nat inside source list 1 pool net200
AC-FS(config)# access-list 1 permit 192.168.12.0 0.0.0.255
```

【Prompt Information】 1: When ip nat outside is configured on the lan port, the configuration fails, prompting:

can't configure this command in lan interface

2: When configuring ip nat inside on the wan port, the configuration fails, prompting:

can't configure this command in wan interface

3: When executing no ip nat outside on the interface configured with ip nat inside, the configuration fails, prompting:

% Interface is outside enabled, try <no ip nat outside>

4: When executing no ip nat inside on the interface configured with ip nat outside, the configuration fails, prompting:

% Interface is inside enabled, try <no ip nat inside>

【Common Mistake】-

【Platform Description】 -

12.3ip nat application

To implement special applications of NAT.

ip nat application source list list-num destination dest-ip { dest-change ip-addr | src-change ip-addr }

ip nat application source list list-num destination { tcp dest-ip port-num | udp dest-ip port-num}

{ dest-change ip-addr port-num | src-change ip-addr port-num }

Cancel this special application.

no ip nat application source list list-num destination dest-ip { dest-change ip-addr | src-change ip-addr }

no ip nat application source list list-num destination { tcp dest-ip port-num | udp dest-ip port-num }

{ dest-change ip-addr port-num | src-change ip-addr port-num }

【Parameter Description】

Parameter	Description
list-num	Internal local address access list, that is, the source address matching condition of the packet.
dest-ip	Matching the internal global address, that is, the destination address matching condition of the packet, only when the destination address matches the address and the source address matches the access list defined above, the NAT translation record will be created.
tcp dest-ip port-num	Match the internal global address and destination port. Only when the destination address and destination port of the tcp packet match the conditions defined here and the source address matches the access list defined above, the NAT translation record will be created.
udp dest-ip port-num	Match the internal global address and destination port. Only when the destination address and destination port of the udp packet match the conditions defined here and the source address matches the access list defined above, the NAT translation record will be created.
dest-change ip-addr port-num	Modify the destination address and destination port of the packets that meet the conditions.
src-change ip-addr	Modify the source address of the packets that meet the conditions.

【Default Configuration】 This rule is not defined.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 In some advanced applications of NAT, it is necessary to modify the source address or destination address of some specific IP packets. This command can then be used. The following example is to use this command to implement the domain name resolution relay service (DNS relay).

【Configuration Example]】 1: In the following configuration, the hosts in the 192.168.1.0 network segment of the intranet will be allowed to point the DNS server to the IP of the NAT inside interface: 192.168.1.1, and the NAT function that supports the NAT device will be responsible for the DNS requests of the intranet hosts. Forward to the real DNS server 202.101.98.55, and forward the DNS response message to the intranet host. Use the ip nat application command to implement this function. The semantics is that if there is a UDP packet whose source address satisfies access-list 1, destination address is 192.168.1.1, and destination port is 53, then modify the destination address of this IP packet to 202.101 .98.55, the destination port is 53.

```
AC-FS#configure terminal
AC-FS(config)# interface GigabitEthernet 0/0
AC-FS(config-if-GigabitEthernet 0/0)# ip address 192.168.1.1 255.255.255.0
AC-FS(config-if-GigabitEthernet 0/0)# ip nat inside
AC-FS(config-if-GigabitEthernet 0/0)# exit AC-
FS(config)# interface GigabitEthernet 0/1
AC-FS(config-if-GigabitEthernet 0/1)# ip address 200.168.12.1 255.255.255.0
AC-FS(config-if-GigabitEthernet 0/1)# ip nat outside
AC-FS(config-if-GigabitEthernet 0/1.)# exit
AC-FS(config)# ip nat pool net200 200.168.12.2 200.168.12.10 netmask 255.255.255.0 AC-
FS(config)# ip nat inside source list 1 pool net200
AC-FS(config)# access-list 1 permit 192.168.12.0 0.0.0.255
AC-FS(config)# ip nat application source list 1 destination udp 192.168.1.1 53 dest-change
202.101.98.55 53
AC-FS(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

【Prompt Information】 1. If the configured rule already exists, the configuration fails, and prompts:

```
% Translation already exist
```

2. If there is insufficient memory when configuring this command, the configuration fails, prompting:

```
% create nat rule fail
```

3. If the command that is not configured successfully is deleted, the deletion fails, and it prompts:

```
% Translation not found
```

【Common Mistake】-

【Platform Description】 -

12.4ip nat inside destination

To enable NAT internal destination address translation

ip nat inside destination list access-list-number pool pool-name

Turn off NAT internal destination translation

no ip nat inside destination list access-list-number

【Parameter Description】

Parameter	Description
list access-list-number	The access list defines the internal global address. If the external network accesses the address in the list, the internal global address will be converted to the internal local address defined in the pool. Note that an extended ACL matching the range 100-199 of the virtual IP should be used here.
pool pool-name	The address pool defines the space for internal local addresses, from which internal local addresses will be allocated during target address translation.

【Default Configuration】 Internal source address translation is not enabled.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Internal destination address translation, which can be used to achieve load balancing of TCP traffic. When a host on the internal network is overloaded with TCP traffic, multiple hosts may be required to balance the load of TCP services. At this time, you can consider using NAT to achieve load balancing of TCP traffic. NAT creates a virtual host to provide TCP services. The virtual host corresponds to multiple internal hosts, and then polls and replaces the target address to achieve load distribution. the goal of. But for other IP traffic, no changes are made unless NAT is configured otherwise.
Configure NAT to implement TCP load balancing. The address of the internal network can be a legal global address or a private network address. But the virtual host address must be a valid global address.

【Configuration Example]】 1: In the following configuration example, the internal network provides a virtual host address 10.10.10.100 to the outside world, and the external network accesses the WWW service through this address. The internal LAN actually provides services with two addresses at 10.10.10.1 and 10.10. 10.2 host. During NAT translation, load balancing is implemented in a round-robin manner.

```
AC-FS#configure terminal
AC-FS(config)# interface GigabitEthernet 0/0
AC-FS(config-if-GigabitEthernet 0/0)# ip address 10.10.10.254 255.255.255.0
AC-FS(config-if-GigabitEthernet 0/0)# ip nat inside
AC-FS(config-if-GigabitEthernet 0/0)# exit AC-
FS(config)# interface GigabitEthernet 0/1
AC-FS(config-if-GigabitEthernet 0/1)# ip address 200.168.12.17 255.255.255.0
```

【Prompt Information】 1: If the configured rule already exists, the configuration fails, prompting:

Translation with list xxx exist,please delete and recreate

2: If there is insufficient memory when configuring this command, the configuration fails, prompting:

% create nat rule fail

3: If the command that is not configured successfully is deleted, the deletion fails, and it prompts:

% Translation not found

【Common Mistake】-

【Platform Description】 -

12.5ip nat inside source

To enable internal source address NAT

ip nat inside source list access-list-number { interface interface-type interface-number | pool pool-name } [overload]

ip nat inside source static local-ip global-ip [match interface-type interface-number | netmask mask][permit-inside]

ip nat inside source static local-ip interface interface-type interface-number [permit-inside]

ip nat inside source static { tcp local-ip local-port | udp local-ip local-port } global-ip global-port [match interface-type interface-number | netmask mask] [permit-inside]

ip nat inside source static { tcp local-ip local-port | udp local-ip local-port } interface interface-type interface-number global-port [permit-inside]

Turn off internal source address NAT.

no ip nat inside source list access-list-number

no ip nat inside source static local-ip global-ip

no ip nat inside source static local-ip interface interface-type interface-number

no ip nat inside source static { tcp local-ip local-port | udp local-ip local-port } global-ip global-port

no ip nat inside source static { tcp local-ip local-port | udp local-ip local-port } interface interface-type interface-number global-port

【Parameter Description】

Parameter	Description
list access-list-number	Local address access list. Only traffic whose source address matches this access list will create a NAT translation record.
Interface interface-type interface-number	Use the global address of the outside interface to do NAPT (Network Address Port Translation), also called extended NAT.
pool pool-name	Use the global address in the address pool for NAT.
overload	Each global address in the pool can be multiplexed and converted, that is, NAPT. This Parameter is not currently configured, and the global address is also multiplexed. The reason for adding this Parameter is to be compatible with cisco commands.
static local-ip global-ip	Define simple static NAT. local-ip is the local address and global-ip is the global address.
static protocol	Define extended static NAT. protocol can be TCP or UDP.
local-port	The service port number for the local address. The port number of TCP or UDP, each service generally corresponds to a service port.
global-port	The service port number for the global address. The external network accesses the service of the internal network host through this port.
permit-inside	Appears only in the ip nat inside source static command to allow intranet users to access local-ip hosts with global-ip.
match interface-type interface-number	Specifies the outgoing interface (used in smart DNS).

【Default Configuration】 No internal source address NAT occurs.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 When the IP address of the internal network is a private address and communication with the external network is required, NAT needs to be configured to convert the internal private IP address into a globally unique IP address.

For some Internet cafes or enterprise units, if only to access the resources of the external network on the Internet, such as browsing web pages, sending and receiving emails, downloading files, etc., but does not provide network services to the external network, you can directly use the IP address of the outside interface as a global address to Address translation is implemented in NAPT mode. If NAT is not performed, even though the internal network that allocates private addresses is physically interconnected with the external network, it cannot communicate with each other because the external network does not have network routes for private addresses.

For internal hosts providing services, static NAT or NAPT needs to be configured. Considering the sustainability of service provision, try not to use the address of the outside interface for static NAPT, because this address is the address interconnected with the ISP, and there is a high possibility of change. Under normal circumstances, intranet users only need to use the intranet IP to access the services provided by these internal hosts. However, some special application services require intranet users to access the service with a global IP. In this case, when configuring internal source address static NAT or internal source address static NAPT, you need to add the permit-inside keyword. At this time, it is best to add no ip redirects to the inside port to prevent the inside port from sending redirected packets.

【Configuration Example]】 1: The following configuration example can dynamically convert the 192.168.12.0/24 internal host to the global address 200.168.12.0/28 network segment. Hosts on other network segments of the internal network are not allowed to do NAT.

```
AC-FS#configure terminal
AC-FS(config)# interface GigabitEthernet 0/0
AC-FS(config-if-GigabitEthernet 0/0)# ip address 192.168.12.6 255.255.255.0
AC-FS(config-if-GigabitEthernet 0/0)# ip nat inside
AC-FS(config-if-GigabitEthernet 0/0)# exit AC-
FS(config)# interface GigabitEthernet 0/1
AC-FS(config-if-GigabitEthernet 0/1)# ip address 200.168.12.17 255.255.255.0
AC-FS(config-if-GigabitEthernet 0/1)# ip nat outside
AC-FS(config-if-GigabitEthernet 0/1)# exit
AC-FS(config)# ip nat pool net200 200.168.12.1 200.168.12.15 prefix-length 28 AC-FS(config)#
ip nat inside source list 1 pool net200
AC-FS(config)# access-list 1 permit 192.168.12.0 0.0.0.255
```

【Prompt Information】 1: When the IP address to be matched in the configuration rule has been mapped, the configuration fails, and the prompt:

```
x.x.x.x already mapped (x.x.x.x -> y.y.y.y)
```

2: When the IP address to be matched in the configuration rule is mapped to the interface address, and the corresponding interface does not exist, the configuration fails, and the prompt:

```
x.x.x.x already mapped
```

3: When the target IP address to be converted in the configuration rule has been mapped, the configuration fails, and the prompt:

```
x.x.x.x.x already mapped (y.y.y.y -> x.x.x.x)
```

4: When the target interface to be converted of the configuration rule has been mapped, the configuration fails, and the prompt:

```
Interface xxx already mapped
```

5: When the configured acl has been mapped, the configuration fails, prompting:

```
Translation with list xxx exist,please delete and recreate
```

6: If there is insufficient memory when configuring this command, the configuration fails, prompting:

```
% create nat rule fail
```

7: If there is insufficient memory when generating subsidiary rules, the configuration fails, prompting:

```
% create attach rule fail
```

8: If there is insufficient memory when configuring the subsidiary rules generated by the permit-inside command, the configuration fails, prompting:

```
% create permit_inside attach rule fail
```

9: If the command that is not configured successfully is deleted, the deletion fails, and it prompts:

```
% Translation not found
```

【Common Mistake】-

【Platform Description】 -

12.6ip nat outside source

To enable external source address NAT

ip nat outside source list access-list-number pool pool-name

ip nat outside source static global-ip local-ip

ip nat outside source static { tcp global-ip global-port | udp global-ip global-port } local-ip local-port

Turn off external source address NAT

no ip nat outside source list access-list-number

no ip nat outside source static global-ip local-ip

no ip nat outside source static { tcp global-ip global-port | udp global-ip global-port } local-ip local-port

【Parameter Description】

Parameter	Description
list access-list-number	Local address access list. Only traffic whose source address matches this access list will create a NAT translation record.
pool pool-name	Use the global address in the address pool for NAT.
static local-ip global-ip	Define simple static NAT. local-ip is the local address and global-ip is the global address.
static protocol	Define extended static NAT. protocol can be TCP or UDP.
local-port	The service port number for the local address. The port number of TCP or UDP, each service generally corresponds to a service port.
global-port	The service port number for the global address. The external network accesses the service of the internal network host through this port.

【Default Configuration】 No external source address NAT occurs.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 External source address NAT translation is mainly applied to address translation in overlapping address spaces. Two private networks that need to be interconnected are assigned the same IP address, or a private network and a public network are assigned the same global IP address. This situation is called address overlap. Communication between two network hosts with overlapping addresses is impossible because they think each other's hosts are on the local network. Overlapping address NAT is specifically aimed at the problem of communication between overlapping address networks. When overlapping address NAT is configured, the external network host address appears as another network host address on the internal network, and vice versa. The

overlapping address NAT configuration is actually divided into two parts: 1) Internal source address NAT configuration; 2) External source address NAT configuration, only the external network overlapping with the internal network address needs to configure external source address translation, and external source address translation can be Use static NAT configuration or dynamic NAT configuration.

When a non-registered global IP address is allocated during the construction of the internal network, and the connection to the Internet is realized, the address overlap will inevitably occur. Internal networks generally use domain names to access external network hosts, so devices that support NAT must also support NAT of DNS packets.

【Configuration Example]】1: The following configuration example, the internal network 192.168.12.0/24 and the external network address overlap. After conversion, the internal host can access the host on the 192.168.12.0/24 network segment of the external network through the 192.168.12.0/24 network address.

```
AC-FS#configure terminal
AC-FS(config)# interface GigabitEthernet 0/0
AC-FS(config-if-GigabitEthernet 0/0)# ip address 192.168.12.55 255.255.255.0
AC-FS(config-if-GigabitEthernet 0/0)# ip nat inside
AC-FS(config-if-GigabitEthernet 0/0)# exit
AC-FS(config)# interface Serial 10/1
AC-FS(config-if-GigabitEthernet 0/1)# ip address 192.168.10.1 255.255.255.0
AC-FS(config-if-GigabitEthernet 0/1)# ip nat outside
AC-FS(config-if-GigabitEthernet 0/1)# encapsulation ppp
AC-FS(config-if-GigabitEthernet 0/1)# exit
AC-FS(config)#ip nat pool net200 200.168.12.1 200.168.12.15 prefix-length 28 AC-
FS(config)#ip nat pool net192 192.168.12.1 192.168.12.254 prefix-length 24 AC-FS(config)#ip
nat inside source list 1 pool net200
AC-FS(config)#ip nat outside source list 1 pool net192 AC-
FS(config)#access-list 1 permit 92.168.12.0 0.0.0.255
AC-FS(config)#ip route 192.168.12.0 255.255.255.0 192.168.100.2
```

【Prompt Information】1: When the IP address to be matched in the configuration rule has been mapped, the configuration fails, and the prompt:

```
6.6.6.6 already mapped (6.6.6.6 -> 5.5.25.4)
```

2: When the target IP address to be converted of the configuration rule has been mapped, the configuration fails, and the prompt:

```
5.5.25.4 already mapped (6.6.6.6 -> 5.5.25.4)
```

3: When the configured acl has been mapped, the configuration fails, prompting:

```
Translation with list 1 exist,please delete and recreate
```

4: If there is insufficient memory when configuring this command, the configuration fails, prompting:

% create nat rule fail

5: If the command that is not configured successfully is deleted, the deletion fails, and it prompts:

% Translation not found

【Common Mistake】-

【Platform Description】 -

12.7ip nat pool

address pool to define NAT.

ip nat pool pool-name start-ip end-ip { netmask netmask | prefix-length prefix-length } [type rotary]

ip nat pool pool-name { netmask netmask | prefix-length prefix-length } [type rotary]

ip nat pool pool-name { netmask netmask | prefix-lengthprefix-length } [type rotary]

delete address pool.

no ip nat pool pool-name

【Parameter Description】

Parameter	Description
pool-name	NAT address pool name.
start-ip	The starting IP address of the NAT address pool.
end-ip	The ending IP address of the NAT address pool.
netmask netmask	The address netmask of the NAT address pool.
type	Type of NAT address pool. Rotary is a rotary type, and each address is assigned an equal probability. Whether it is equipped with rotary is all rotary. The reason why the rotary Parameter is introduced is to be compatible with the cisco command.

【Default Configuration】 No address pool is defined.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 If an address pool needs to define multiple address blocks, you need to create an empty address pool first, and then define the address range.

【Configuration Example]】1: The following configuration example creates an address pool named net192, the starting address is 192.168.12.1, the ending address is 192.168.12.254, and the netmask length is 24 bits.

```
AC-FS#configure terminal
AC-FS(config)# ip nat pool net192 192.168.12.1 192.168.12.254 prefix-length 24
```

【Prompt Information】 1: If the mask of the configured address pool is 0.0.0.0, the configuration fails, and a prompt is displayed.

```
% netmask can not be 0
```

2: If the end IP address configured by this command is smaller than the start IP address, the configuration fails, and the prompt:

```
% End address less than start address
```

3: If the start IP address and end IP address configured by this command are not in the same network segment, the configuration fails, and prompts:

```
% Start and end addresses on different subnets
```

4: If the start IP address and end IP address configured by this command are both 0.0.0.0, the configuration fails, prompting:

```
% Ip address 0.0.0.0 ~ 0.0.0.0 are invalid.
```

5: If the pool type entered into the corresponding address pool mode is different from the configured pool type, the configuration fails, prompting:

```
%Cannot redefine pool type, please delete and recreate.
```

6: If the number of configured address pools exceeds 100, the configuration fails, prompting:

```
% Exceed the max pool count
```

7: If the name of the configured address pool exceeds 32, the configuration fails, prompting

```
% Length of pool name must be no more than 32 charceters
```

8: If the memory is insufficient when configuring this command, the configuration fails, and prompts:

```
%create pool fail
```

9: If the memory is insufficient when configuring this command, the configuration fails, prompting:

```
% create pool fail for alloc range mem
```

10: If the address pool to be deleted does not exist, the deletion fails and prompts:

```
% pool xxx not exist
```

【Common Mistake】-

【Platform Description】 -

12.8ip nat keepalive

To configure the interval for sending NAT native address free arp packets.

ip nat keepalive [keealive_out]

Do not send free arp packets to the NAT local address.

no ip nat keepalive default ip nat keepalive

【Parameter Description】

Parameter	Description
keealive_out	Interval for sending free arp messages of nat local address.

【Default Configuration】 Do not send free arp messages of nat local address.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】NAT needs to treat the addresses in some configuration rules as the local address. To prevent address conflicts, you can solve the problem by sending free arp packets regularly.

【Configuration Example]】1: The following configuration example, set the time interval for sending nat local address to 10s

```
AC-FS#configure terminal
AC-FS(config)# ip nat keepalive 10
```

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

12.9ip nat translation

alg to configure NAT support.

ip nat translation { dns [ttl ttl_time] | ftp [port port_num] | tftp | pptp | h323 | rtsp }

Remove alg for NAT support.

no ip nat translation { dns | ftp | tftp | pptp | h323 | rtsp }

【Parameter Description】

Parameter	Description
ttl	Defines the timeout for UDP connection translation records applied by DNS. Default is 0.
port_num	Define the port number that supports ftp applications, the default is 21.

【Default Configuration】Open alg that supports dns/ftp/tftp/pptp/h323/rtsp

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 ALG (Application Level Gateway) mainly completes the processing of application layer packets. Normally, NAT only converts the IP address and port information in the packet header, and does not analyze the Field in the application layer data payload. However, for some special protocols, such as ftp/dns/tftp, the data payload of their packets may contain IP address or port information. These contents cannot be effectively translated by NAT, which may cause problems. The NAT ALG technology can perform the analysis and address translation of application layer message information for multi-channel protocols, and perform corresponding translation and processing of IP addresses and ports that need address translation in the payload or fields that need special processing, so as to ensure the application layer. correctness of communication.

For example, the FTP application is completed by the data connection and the control connection, and the establishment of the data connection is dynamically determined by the payload field information in the control connection, which requires application layer protocol detection to complete the conversion of the payload field information to ensure subsequent data. The connection is established correctly.

【Configuration Example]】1: The following configuration example, set the dns cache time to 30s.

```
AC-FS#configure terminal
AC-FS(config)# ip nat translation dns ttl 30
```

2: The following configuration example supports port 25 for ftp applications.

```
AC-FS#configure terminal
AC-FS(config)# ip nat translation ftp port 25
```

【Prompt Information】 1: Successfully delete the corresponding alg, prompt:

unregister xxx alg success!

2: Deleting the corresponding alg fails, prompting:

unregister xxx alg fail!

3: Successfully support the corresponding alg, prompt:

register xxx alg success!

4: Failed to support the corresponding alg, prompt:

register xxx alg fail!

【Common Mistake】-

【Platform Description】 -

12.10show ip nat translations

Displays NAT translation records.

show ip nat translations [dev_id] [slot_id] [acl_num] [icmp | tcp | udp] [verbose]

【Parameter Description】

Parameter	Description
icmp	Show only nat conversion records for icmp.
tcp	Only show nat conversion records for tcp.
udp	Show only nat conversion records for udp.
acl_num	acl number, only supports extended acl, used to filter the display content
verbose	Displays more detailed NAT translation log information.
dev_id	Device ID

slot_id	Slot ID of business card

【Command Mode】 Privileged mode

【Default Level】 1

【Usage Guide】 This command can display the summary of IP NAT translation records, such as protocol, internal global address and port number, internal local address and port number, external local address and port number, external global address and port number. Follow the verbose Parameter to display more detailed information, including the set timeout time, the remaining time of the record, the record mark, etc.

【Configuration Example]】 1: Display NAT translation records:

```
AC-FS# show ip nat translations verbose
timeout for NAT TCP flows: 86400
timeout for NAT TCP flows after a FIN or RST: 60
timeout for NAT TCP flows after a SYN : 60
timeout for NAT UDP flows: 300
timeout for NAT DNS flows: 60
timeout for NAT ICMP flows: 60
Pro Inside global      Inside local       Outside local      Outside global timeout vrf
tcp 192.168.5.103:1987 192.168.211.21 :1987 211.67.71.7    :80.....211.67.71.7:80 timeout=85139 1
udp 192.168.5.103:1041 192.168.211.183:1041 202.101.98.55  :53 202.101.98.55:53 timeout=38 1
```

Field Description:

Field	Description
Pro	agreement type. "udp" indicates that the conversion record is a UDP conversion record; "tcp" indicates that the conversion record is a TCP conversion record. "icmp" indicates that the conversion record is an ICMP conversion record.
Inside global	Internal global address and port number.
Inside local	Internal local address and port number.
Outside local	External local address and port number.
Outside global	External global address and port number.
timeout	Indicates how long the NAT translation record is before the timeout, in seconds.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

13 DDNS

13.1peanut username password

Set the peanut shell account password.

peanut username username password password

Cancel the peanut shell account password.

no peanut username

【Parameter Description】

Parameter	Description
username username	Peanut shell account.
password password	Peanut Shell Code.

【Default Configuration】 No peanut shell account password is configured.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】After configuring the peanut shell account password, the device will automatically connect with the peanut shell server, and bind the device IP and domain name.

【Configuration Example]】1: Configure peanut shells.

```
AC-FS#configure terminal
AC-FS (config)# peanut username AC-FS password AC-FS
```

【Verification】1: Use the show peanutinfo command to view the peanut shell account password and connection status.

【Prompt Information】-

【Common Mistake】 1: The password of the peanut shell account is wrong.

2: The device is not properly configured with DNS and cannot correctly resolve the peanut shell server IP.

3: The peanut shell server is unreachable.

【Platform Description】 -

13.2peanut serverinfo key

Set peanut shell server information.

peanut server servername info infovalue key keyvalue

Cancel peanut shell server information.

no peanut server

【Parameter Description】

Parameter	Description
server servername	Peanut shell server URL.
info infovalue	peanut shell info value.
key keyvalue	Peanut shell key value.

【Default Configuration】 No peanut shell server information is configured.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 After configuring the peanut shell server information, after configuring the peanut shell account password, the device will automatically connect to the designated peanut shell server, and the device IP

tied to the domain name.

【Configuration Example]】1: Configure peanut shells.

```
AC-FS#configure terminal
AC-FS (config)# peanut server hph019.oray.net info 0X26A09899 key 0X1E0808B7
```

【Verification】1: Use the show peanutinfo command to view the configuration information of the peanut shell server.

【Prompt Information】-

【Common Mistake】 1: The URL or info and key values of the peanut shell server are wrong.

2: The device is not properly configured with DNS and cannot correctly resolve the peanut shell server IP.

3: The peanut shell server is unreachable.

【Platform Description】 -

13.3show peanutinfo

Check the peanut shell account password and connection status.

show peanutinfo

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode, global mode

【Default Level】 14

【Usage Guide】 Use this command to view the peanut shell account password and connection status on the device.

【Configuration Example]】 1: View the peanut shell account password and connection status on the device.

```
AC-FS#show   peanutinfo
peanut   state:   success
peanut   username:AC-FS
peanut password:AC-FS
peanut_server:hph019.oray.net
peanut_info:0X26A09899
peanut_key:0X1E0808B7
```

Field Description:

Field	Description
peanut state	Connection Status.
peanut username	Account.
peanut password	Password.
peanut_server	Server URL..

peanut_info	info value.
peanut_key	key value.

【Prompt Information】-

【Platform Description】 -

Chapter 8 IP Routing

This volume introduces the contents of the IP Routing Command Manual, including the following chapters:

1. The protocol is irrelevant
2. NSM
3. FRM
4. ROUTE-DB

1 protocol irrelevant

1.1accept-lifetime

Configure the lifetime for the receive direction of the keychain.

accept-lifetime start-time { infinite | end-time | duration seconds }

Removes the lifetime for the receive direction of the keychain.

no accept-lifetime

【Parameter Description】

Parameter	Description
start-time	Specifies the start time of the lifetime.
infinite	This Parameter indicates that the key is valid from the start time.
end-time	The end time of the key validity period, which must be later than start-time.
duration seconds	Specifies the duration of the validity period starting from start-time, the value range: 1-2147483646.

【Default Configuration】 The keychain receiving lifetime is not defined

【Command Mode】Keychain key configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure keychain kc, enter keychain configuration mode, configure key1, enter key1 configuration mode, and define keychain reception lifetime

```
AC-FS(config)#key chain kc AC-
FS(config-keychain)#key 1
AC-FS(config-keychain-key)#key-string Hello
AC-FS(config-keychain-key)#accept-lifetime 16:30:00 Oct 1 2010 duration 43200
```

【Verification】1: Use the show running-config command to view the configuration.

【Common Mistake】-

【Platform Description】 -

1.2ip as-path access-list

Defines AS path filtering rules based on regular expressions.

ip as-path access-list path-list-num { permit | deny } regular-expression

Remove regex-based AS path filtering rules.

no ip as-path access-list path-list-num [{ permit | deny } regular-expression]

【Parameter Description】

Parameter	Description
path-list-num	AS path control list name based on regular expression, AS path list identifier, range: 1---500.
permit	allow access.
deny	access denied.
regular-expression	Regular expression. Range: 1..255 characters.

【Default Configuration】 No definition list

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 For the introduction of regular expressions, please refer to the configuration guide.

【Configuration Example]】1: Create an AS path filtering rule to match path information that only contains AS number 123.

```
AC-FS(config)# ip as-path access-list 105 deny ^123$
```

【Verification】1: Use the show running-config command to view the configuration.

2: Use the show ip bgp filter-list command to filter whether the policy takes effect.

【Prompt Information】1: When deleting an AS path filter rule, if the entered rule name or filter rule does not exist, an error message will be displayed.

```
% This object doesn't exist
```

2: If an invalid filter rule is entered, an error message will be displayed.

% Can't compile regexp

3: If the AS path filtering rule with duplicate rules is configured, an error message will be displayed.

% Insertion failed with duplicate policy

【Common Mistake】-

【Platform Description】 -

1.3ip community-list

Define a list of community attributes.

Defines a list of community attributes for standard types and controls access to it.

ip community-list { community-list-number | standard community-list-name } { permit | deny } [{ community-list-number | internet | local-AS | no-advertise | no-export }]

Defines a list of community attributes for the extension type and controls access to it.

ip community-list { community-list-number | expanded community-list-name } { permit | deny } [regular-expression]

Delete the list of community attributes.

no ip community-list { { standard | expanded } community-list-name | community-list-number }

【Parameter Description】

Parameter	Description
standard	List of Standards Groups.
expanded	Extended group list.
community-list-name	group list name Group list name must not exceed 80 characters
community-list-number	group list number List of Standard Groups: Numbers in the range 1-99 Extended community list: numbering range 100-199
permit	allow access.
deny	access denied.
community-number	Community attribute value. The format is AA:NN (autonomous system number: 2-byte number), or a numeric value in the range 0-4294967295.

internet	Indicates the Internet community to which all paths belong.
local-AS	Indicates that this path is not advertised to the outside of this AS. When confederation is configured, this path is not advertised to other autonomous systems or sub-ASs.
no-advertise	Indicates that this path does not publish any BGP peers.
no-export	Indicates that this path is not published to EBGP peers.

【Default Configuration】 No group list is defined

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to define the community list for BGP.

Currently each community list can support up to 32 community values, including internet, local-AS, no-advertise and no-export.

【Configuration Example]】 1: Define a list of standard community attributes, and reject community attributes 100:20 and 200:20.

```
AC-FS(config)# ip community-list standard test deny 100:20 200:20
```

2: Define a list of standard community attributes, allowing community attributes internet.

```
AC-FS(config)# ip community-list standard test2 permit internet
```

【Verification】 1: Use the show running-config command to view the configuration.

【Prompt Information】 1: If the specified community attribute list name is all numbers, it will prompt an error message.

```
% Community-list name cannot have all digits
```

2: If the length of the specified community attribute list name exceeds 80 characters, an error message will be displayed.

```
% Community-list name lengths should be less than 80 chars
```

3: When deleting, if the input list or filter rule does not exist, an error message will be prompted.

```
% This object doesn't exist
```

4: If a community attribute filtering rule with duplicate rules is configured, an error message will be displayed.

```
% Insertion failed with duplicate policy
```

5: If a community attribute filtering rule with duplicate serial numbers is configured, an error message will be displayed.

```
% Community-list entry with this sequence already exist
```

6: If the standard and extended community attribute lists with the same name are defined at the same time, an error message will be prompted.

```
% Community-list name conflict with previous defined
```

【Common Mistake】-

【Platform Description】 -

1.4ip extcommunity-list

Define the extended community attribute list referenced in the Route Map. The Route Map associated with this list will be used to control the filtering of VPN routes in BGP/MPLS VPN applications.

ip extcommunity-list {expanded-list | expanded list-name } { permit | deny } [regular-expression]

A list of extended community attributes that define standard types.

ip extcommunity-list {standard-list | standard list-name } { permit | deny } [rt value] [soo value]

Remove extended community attribute list.

no ip extcommunity-list {expanded-list | expanded list-name | standard-list | standard list-name }

The created extended community attribute list, you can enter the configuration mode of ip extcommunity-list.

ip extcommunity-list {expanded-list | expanded list-name| standard-list | standard list-name }

Remove the extended property list.

no ip extcommunity-list {expanded-list | expanded list-name | standard-list | standard list-name}

【Parameter Description】

Parameter	Description
expand-list	The value range is [100~199], which is used to identify the extended extcommunity list. An extcommunity list can contain multiple rules.
standard-list	The value range is [1~99], which is used to identify the standard extcommunity list. An extcommunity table can contain multiple rules.

expanded list-name	The name of the extended extcommunity, using this parameter will enter the configuration mode of the extended community attribute list. The name must be no more than 32 characters long.
standard list-name	The name of the standard extcommunity, used to identify the name of the standard extcommunity table, using this parameter will enter the configuration mode of the extended community attribute list. The name must be no more than 32 characters long.
permit	Define an allowed extcommunity rule.
deny	Define a deny extcommunity rule.
regular-expression	(Optional) Defines a matching template to use against extcommunity.
sequence-number	(Optional) Defines the sequential sequence number for this rule, ranging from 1 to 2147483647. If not specified, by default, the serial number of each additional rule is automatically incremented by 10, and the numbering starts from 10.
rt	(Optional) Set RT property value, this command can only be used in standard extcommunity configuration, not in extended extcommunity configuration.
soo	(Optional) Set the SOO property value. This command can only be used in standard extcommunity configuration, not in extended extcommunity configuration.
value	The value of the extended community (extend_community_value) extend_community_value can have three different Parameter: extend_community_value=as_num:nn. an_num is the public autonomous domain system number (2-byte AS), nn is defined by the user, and the range is 0..4294967295. extend_community_value=ip_addr:nn. The ip_addr address must be a global IP address, nn is defined by the user, and the range is 0..65535.
	= extend_community_value=as4_num:nn. an4_num is the public autonomous domain system number (4-byte AS), nn is defined by the user, the range is 1..65535 In version 10.4(3) or later, 4-byte AS number is added, that is, the new AS number range is 1..4294967295, which is represented as 1..65535.65535 in dot mode.

【Default Configuration】 The extended community attribute list rule is not defined by default.

【Command Mode】 Global configuration mode, ip extcommunity-list configuration mode

【Default Level】 14

【Usage Guide】 The ip extcommunity-list command is used to create an extcommunity rule list with multiple extcommunity values. It is mainly used in the match extcommunity rule of RouteMap to match the extended community attribute of BGP routes to achieve the purpose of route filtering. For the definition of extended extcommunity rules, the rules of its regular-expression are as follows:

Character	Symbol	Special meaning
sentence	.	matches any single character.
Asterisk	*	matches zero or any sequence in a string.
plus	+	Match one or any sequence of strings.
question mark	?	matches zero or one symbol in a string.
plus size	^	matches the beginning of the string.
dollar number	$	Matches the end of the string.
underscore	_	Matches commas, parentheses, beginning and end of strings, spaces.
Square brackets	[]	Match a single character in a range.

The commands in expanded ip extcommunity-list configuration mode are:

[sequence-number]deny regular-expression Defines a deny extcommunity rule. [sequence-number] permit regular-expression Defines a permitted extcommunity rule. exit Exit the current exit mode.

no [sequence-number]deny regular-expression Removes a denied extcommunity rule.

no [sequence-number] permit regular-expression Removes a permit extcommunity rule.

The commands in standard ip extcommunity-list configuration mode are:

[sequence-number] deny {[rt value] [soo value]} Defines a deny extcommunity rule. [sequence-number] permit {[rt value] [soo value]} Defines a permit extcommunity rule. exit Exit the current exit mode.

no [sequence-number] deny {[rt value] [soo value]} Removes a deny extcommunity rule.

no [sequence-number] permit {[rt value] [soo value]} Removes a permit extcommunity rule.

【Configuration Example]】 1: Define ip extcommunity-list:

```
AC-FS(config)# ip extcommunity-list 1 permit rt 100: 1
AC-FS(config)# ip extcommunity-list standard aaa permit rt
100: 2
AC-FS(config)# ip extcommunity-list expanded ext1 permit 200: [0~9][0~9]
```

2: How to use ip extcommunity:

```
AC-FS(config)# route-map rt_in_filter AC-
FS(config-route-map)# match extcommunity 1 AC-
FS(config-route-map)# match extcommunity ext1 AC-
FS(config)# router bgp 100
AC-FS(config-router)# address-family vpn
AC-FS(config-router-af)#neighbor 3.3.3.3 send-community extended AC-
FS(config-router-af)#neighbor 3.3.3.3 route-map rt_in_filter in
```

【Verification】1: Use the show running-config command to view the configuration.

【Prompt Information】 1: When deleting, if the input list or filter rule does not exist, an error message will be prompted.

% This object doesn't exist

2: If the extended community attribute filtering rule with duplicate rules is configured, an error message will be displayed.

% Insertion failed with duplicate policy

3: If an extended community attribute filtering rule with duplicate serial numbers is configured, an error message will be displayed.

% Extcommunity-list entry with this sequence already exist

4: If the standard and extended extended community attribute lists with the same name are defined at the same time, an error message will be prompted.

% Extcommunity-list name conflict with previously defined

【Common Mistake】-

【Platform Description】 -

1.5ip prefix-list

Create a prefix list or add a prefix list entry.

ip prefix-list prefix-list-name [seq seq-number] { deny | permit } ip-prefix [ge minimum-prefix-length] [le maximum-prefix-length]

Delete a prefix list or prefix list entry.

no ip prefix-list prefix-list-name [seq seq-number] { deny | permit } ip-prefix [ge minimum-prefix-length] [le maximum-prefix-length]

【Parameter Description】

Parameter	Description
prefix-list-name	prefix list name.
seq-number	Assign a sequence number to a prefix list entry. Its range is 1 to 2147483647. If the sequence number is not included in the command, the system will assign a default sequence number to this prefix list entry. The default sequence number of the first entry is 5, and the default sequence number value of each subsequent unassigned entry is the value of the first multiple of 5 greater than the previous sequence number.
deny	Deny access for matching cases.
permit	Allow access for matching cases.
ip-prefix	Configure the network address and mask. The mask length is from 0 to 32.
minimum-prefix-length	The specified minimum range value (that is, the starting length of the range) The ge keyword stands for greater than or equal to. When neither ge nor le are set, the mask length must be exactly the same to match the rule.
maximum-prefix-length	The specified maximum range value (i.e. the end length of the range) The le keyword stands for the less than or equal operation. When neither ge nor le are set, the mask length must be exactly the same to match the rule.

【Default Configuration】 No prefix list is created

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 The ip prefix-list command is used to configure IP prefix filtering. Prefix lists use the permit or deny keywords to determine deny and accept actions in case of a match.

Prefix lists are used to define exact or range matches for a prefix. The ge or le keyword is used to define a range of prefixes for matching, providing more flexible matching configuration than simply typing ip-prefix. ip-prefix provides exact prefix range matching if there are no ge or le keywords in the command. If only ge is entered, the matching range is minimum-prefix-length to 32. If only le is entered, the matching range is the mask length of ip-prefix to maximum-prefix-length . If both are entered, the matching range is from minimum-prefix-length to maximum-prefix-length. That is, the relationship between ip-prefix mask, minimum-prefix-length and maximum-prefix-length is: ip-prefix mask length < minimum-prefix-length < maximum-prefix-length <= 32.

【Configuration Example]】 1: Filter the route distribution information output during RIP redistribution in the OSPF protocol according to the destination IP, and the filtering rules are defined in the associated IP prefix list (only routes with the destination IP in the range of 201.1.1.0/24 are allowed) information is distributed).

```
AC-FS# configure terminal
AC-FS(config)# ip prefix-list pre1 permit 201.1.1.0/24 AC-
FS(config)# router ospf
AC-FS(config-router)# distribute-list prefix pre1 out rip
AC-FS(config-router)# end
```

【Verification】 1: Use the show running-config command to view the configuration.

【Prompt Information】 -1: If the configuration rule duplicates the prefix list entry, an error message will be displayed.

```
% Insertion failed with duplicate policy
```

【Common Mistake】 -

【Platform Description】 -

1.6ip prefix-list description

Add the text Description to a prefix list.

ip prefix-list prefix-list-name description description descripton-text

Deletes the Description of a prefix list.

no ip prefix-list prefix-list-name description

【Parameter Description】

Parameter	Description
prefix-list-name	prefix list name.
descripton-text	Prefix list text Description.

【Default Configuration】 No prefix list text Description

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Add the text Description Deny routes from Net-A to the IP prefix list.

```
AC-FS# configure terminal
AC-FS(config)# ip prefix-list pre description Deny routes from Net-A
```

【Verification】1: Use the show running-config command to view the configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.7ip prefix-list sequence-number

Enable sorting for prefix lists.

ip prefix-list sequence-number

Cancel the sorting function of the prefix list.

no ip prefix-list sequence-number

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 The prefix list sorting function is not enabled

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Enable the sorting function for the prefix list.

```
AC-FS# configure terminal
AC-FS(config)# ip prefix-list sequence-number
```

【Verification】1: Use the show running-config command to view the configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.8key

Define a key in the keychain.

key key-id

Delete the key in the keychain.

no key key-id

【Parameter Description】

Parameter	Description
key-id	ID of the authentication key in the keychain, value range: 0-2147483647.

【Default Configuration】 -

【Command Mode】 Keychain configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure keychain ripkeys, enter keychain configuration mode, configure key 1

```
AC-FS(config)# key chain ripkeys
AC-FS(config-keychain)# key 1
```

【Verification】1: Use the show running-config command to view the configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.9 key chain

Define the keychain and enter keychain configuration mode.

key chain key-chain-name

Delete the keychain.

no key chain key-chain-name

【Parameter Description】

Parameter	Description
key-chain-name	Keychain name.

【Default Configuration】-

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 For the keychain to take effect, at least one key must be configured.

【Configuration Example]】1: Configure the keychain ripkeys and enter the keychain configuration mode.

```
AC-FS(config)# key chain ripkeys
```

【Verification】1: Use the show running-config command to view the configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.10 key-string

Specifies the authentication string in the keychain key schema.

key-string [0|7] text

delete key authentication string

no key-string

【Parameter Description】

Parameter	Description
0	Specifies that the key is displayed in clear text.
7	Specifies that the key is displayed in ciphertext.
text	the specified authentication string character.

【Default Configuration】-

【Command Mode】Keychain key configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the keychain ripkeys, enter the keychain configuration mode, configure key 1, enter the key 1 configuration mode, and define the key string as abc.

```
AC-FS(config)# key chain ripkeys
AC-FS(config-keychain)# key 1 AC-FS(config-
keychain-key)# key-string abc
```

【Verification】1: Use the show running-config command to view the configuration.

【Prompt Information】1: If the length of the configured plaintext password is greater than 80 or the length of the ciphertext password is greater than 162, an error message will be prompted.

```
%Error: key string too long
```

2: If the configured ciphertext password does not meet the encryption rules, such as key-string 7 123, an error message will be displayed.

```
% Invalid encrypted password: 123
```

【Common Mistake】-

【Platform Description】 -

1.11match community

COMMUNITY attribute routes allowed in the redistribution access list.

match community { community-list-number | community-list-name } [exact-match] [{ community-list-number | community-list-name } [exact-match] …]

Delete existing configuration.

no match community { community-list-number | community-list-name } [exact-match] [{ community-list-number | community-list-name } [exact-match] …]

【Parameter Description】

Parameter	Description
community-list-number	group list number. List of Standard Groups: Numbers in the range 1-99. Extended community list: numbering range 100-199.
communitys-list-name	group list name. Group list name must not exceed 80 characters.
exact-match	exact match list.

【Default Configuration】-

【Command Mode】 Routing map configuration mode

【Default Level】 14

【Usage Guide】 The match community command can be followed by multiple community list numbers or community list names, but the sum of the two numbers is not greater than 6. Each exact-match keyword modifies only the previous list, not all matching lists.
In a routing map rule configuration, one or more match commands and one or more set commands can be executed. If there is no match command, match all; if there is no set command, do nothing.

【Configuration Example]】1: Configure the routing map, and set the local preference attribute to 20 for the route that exactly matches the community attribute list 1.

```
AC-FS(config)# ip community-list 1 permit 100:2 100:30 AC-
FS(config)# route-map set_lopref
AC-FS(config-route-map)# match community 1 exact-match
AC-FS(config-route-map)# set local-preference 20
```

【Verification】1: Use the show running-config command to view the configuration.

【Prompt Information】 1: If the specified name type Community-list name is all numbers, it will prompt an error message.

```
% Community-list name cannot have all digits
```

2: If the length of the specified Community-list name is more than or equal to 80 characters, an error message will be displayed.

```
% Community-list name lengths should be less than 80 chars
```

3: If there are more than 6 community-list lists configured in a single command, an error message will be displayed.

```
% Match community command only support six community-list
```

4: If the total number of configured Community-list lists exceeds 6, an error message will be displayed.

```
% Match community can't exceed 6!
```

【Common Mistake】-

【Platform Description】 -

1.12 match interface

Match the next hop egress to the specified interface.

match interface interface-type interface-number […interface-type interface-number]

Delete the configuration that matches the next-hop egress as the specified interface.

no match interface [interface-type interface-number […interface-type interface-number]]

【Parameter Description】

Parameter	Description
interface-type	Interface Type.

interface-number	interface number.

【Default Configuration】-

【Command Mode】 Routing map configuration mode

【Default Level】 14

【Usage Guide】 The match interface command can be followed by multiple interfaces.

Routing information can be redistributed from one routing process to another routing process. For example, the routes of the OSPF routing domain can be redistributed and advertised to the RIP routing domain, or the routes of the RIP routing domain can be redistributed and advertised to the OSPF routing domain.

In route redistribution, the mutual distribution of routes between two routing domains is often conditionally controlled through the application of route maps. In a routing map rule configuration, one or more match commands and one or more set commands can be executed. If there is no match command, match all; if there is no set command, do nothing.

The configuration of the routing map is very flexible and can be applied to the configuration of route redistribution and policy routing. No matter how the routing map is applied, the configuration principle is the same, but the applicable command set is different. Even if the same applies to route redistribution, different routing protocols apply routing graphs, and the commands that can be used are different.

By default, if you do not enter the interface type and interface number when deleting a configuration, the configuration of all matching interfaces will be deleted.

【Configuration Example]】1: Configure the OSPF routing protocol to redistribute RIP routes, requiring only the RIP routes whose next hop is GigabitEthernet 0/0 to be redistributed.

```
AC-FS(config)# router ospf
AC-FS(config-router)# redistribute rip subnets route-map redrip
AC-FS(config-router)# network 192.168.12.0 0.0.0.255 area 0 AC-
FS(config-router)# exit
AC-FS(config)# route-map redrip permit 10
AC-FS(config-route-map)# match interface GigabitEthernet 0/0
```

【Verification】1: Use the show running-config command to view the configuration.

【Prompt Information】 1: If the number of specified interfaces exceeds 4, an error message will be displayed.

```
% Match interface can't exceed 4!
```

2: If the specified interface is a Layer 2 port (for example, Layer 2 port GigabitEthernet 0/0), an error message will be displayed.

```
% Invalid parameter: GigabitEthernet 0/0, only support layer 3 interface.
```

【Common Mistake】-

【Platform Description】 -

1.13 match ip address

Redistribute the destination network routes allowed in the access list or prefix list.

match ip address { access-list-number [access-list-number... | access-list-name...] | access-list-name [access-list-number...| access-list-name] | prefix-list prefix-list-name [prefix-list-name...] }

Delete existing configuration.

no match ip address [access-list-number [access-list-number... | access-list-name...] | access-list-name [access-list-number... | access-list-name] | prefix-list prefix-list-name [prefix-list-name...]]

【Parameter Description】

Parameter	Description
access-list-number	Access list number. Standard access list number range: 1-99, 1300-1999. Extended access list number range: 100-199, 2000-2699.
access-list-name	access list name.
prefix-list prefix-list-name	prefix list names to match.

【Default Configuration】-

【Command Mode】 Routing map configuration mode

【Default Level】 14

【Usage Guide】 The match ip address command can be followed by multiple access list numbers or access list names. Routing information can be redistributed from one routing process to another routing process. For example, the routes of the OSPF routing domain can be redistributed and advertised to the RIP routing domain, or the routes of the RIP routing domain can be redistributed and advertised to the OSPF routing domain. Mutual redistribution of routes is possible among all IP routing protocols. In route redistribution, the mutual distribution of routes between two routing domains is often conditionally controlled through the application of route maps. In a routing map rule configuration, one or more match commands and one or more set commands can be executed. If there is no match command, match all; if there is no set command, do nothing.

The configuration of the routing map is very flexible and can be applied to the configuration of route redistribution and policy routing. No matter how the routing map is applied, the configuration principle is the same, but the applicable command set is different. Even if the same applies to route redistribution, different routing protocols apply routing graphs, and the commands that can be used are different. By default, deleting a configuration without entering a list number will delete all lists.

【Configuration Example]】1: Configure the OSPF routing protocol to redistribute RIP routes, requiring only the RIP routes that meet access list 10 to be redistributed. In the OSPF routing domain, the route type is external route type-1, and the initial metric value is 40.

```
AC-FS(config)# router ospf
AC-FS(config-router)# redistribute rip subnets route-map redrip
AC-FS(config-router)# network 192.168.12.0 0.0.0.255 area 0 AC-
FS(config-router)# exit
AC-FS(config)# access-list 10 permit 200.168.23.0 0.0.0.255 AC-
FS(config)# route-map redrip permit 10
AC-FS(config-route-map)# match ip address 10
AC-FS(config-route-map)# set metric 40
AC-FS(config-route-map)# set metric-type type-1
```

【Verification】1: Use the show running-config command to view the configuration.

【Prompt Information】 1: If the specified ACL name is invalid (for example, match ip address 12345), an error message will be displayed.

```
% ACL name 12345 is invalid
```

2: If the matching prefix-list has been configured before, and then the matching ACL is configured, an error message will be displayed.

```
% Can't set access-list match with prefix-list exits!
```

3: If the matching ACL has been configured before, and the matching prefix-list is configured again, an error message will be displayed.

```
% Can't set prefix-list match with access-list exists!
```

4: If the number of ACLs specified by a single command exceeds 6, an error message will be displayed.

```
% Match ip address command only support six IP access-list
```

5: If there are more than 6 ACLs configured in total, an error message will be displayed.

```
% ACL can't exceed 6!
```

6: If the number of prefix-lists specified in a single command exceeds 6, an error message will be displayed.

```
% Match ip address command only support six IP prefix-list
```

7: If there are more than 6 prefix-lists configured in total, an error message will be displayed.

```
% Prefix-list can't exceed 6!
```

【Common Mistake】-

【Platform Description】 -

1.14 match ip next-hop

Redistribute destination network routes whose next-hop IP addresses match the access list or prefix list rules.

match ip next-hop { access-list-number [access-list-number... | access-list-name...] | access-list-name [access-list-number... | access-list-name] | prefix-list prefix-list-name [prefix-list-name...] }

Delete existing configuration.

no match ip next-hop [access-list-number [access-list-number... | access-list-name...] | access-list-name [access-list-number... | access-list-name] | prefix-list prefix-list-name [prefix-list-name...]]

【Parameter Description】

Parameter	Description
access-list-number	access list number. Standard access list number range: 1-99, 1300-1999. Extended access list number range: 100-199, 2000-2699.
access-list-name	access list name.
prefix-list prefix-list-name	prefix list names to match.

【Default Configuration】-

【Command Mode】 The routing map configuration mode.

【Default Level】 14

【Usage Guide】 The match ip next-hop command can be followed by multiple access list numbers or access list names. Routing information can be redistributed from one routing process to another routing process. For example, it can redistribute the OSPF routing domain process to another routing process. For example, the routes of the OSPF routing domain can be redistributed and advertised to the RIP routing domain, or the routes of the RIP routing domain can be redistributed and advertised to the OSPF routing domain. Mutual redistribution of routes is possible among all IP routing protocols.

In route redistribution, the mutual distribution of routes between two routing domains is often conditionally controlled through the application of route maps. In a routing map rule configuration, one or more match commands and one or more set commands can be executed. If there is no match command, match all; if there is no set command, do nothing.

By default, deleting a configuration without entering a list number will delete all lists.

【Configuration Example]】1: Configure the OSPF routing protocol to redistribute RIP routes. OSPF allows redistribution of a RIP route as long as its next-hop address matches access list 10 or 20.

```
AC-FS(config)# router ospf
AC-FS(config-router)# redistribute rip subnets route-map redrip
AC-FS(config-router)# network 192.168.12.0 0.0.0.255 area 0
AC-FS(config-router)# exit
```

```
AC-FS(config)# access-list 10 permit host 192.168.10.1 AC-
FS(config)# access-list 20 permit host 172.16.20.1 AC-FS(config)#
route-map redrip permit 10
AC-FS(config-route-map)# match ip next-hop 10 20
```

【Verification】1: Use the show running-config command to view the configuration.

【Prompt Information】1: If the specified ACL name is invalid (for example, match ip next-hop 12345), an error message will be displayed.

```
% ACL name 12345 is invalid
```

2: If the matching prefix-list has been configured before, and then the matching ACL is configured, an error message will be displayed.

```
% Can't set access-list match with prefix-list exits!
```

3: If the matching ACL has been configured before, and the matching prefix-list is configured again, an error message will be displayed.

```
% Can't set prefix-list match with access-list exists!
```

4: If the number of ACLs specified by a single command exceeds 6, an error message will be displayed.

```
% Match ip next-hop command only support six IP access-list
```

5: If there are more than 6 ACLs configured in total, an error message will be displayed.

```
% ACL can't exceed 6!
```

6: If the number of prefix-lists specified in a single command exceeds 6, an error message will be displayed.

```
% Match ip next-hop command only support six IP prefix-list
```

7: If there are more than 6 prefix-lists configured in total, an error message will be displayed.

```
% Prefix-list can't exceed 6!
```

【Common Mistake】-

【Platform Description】 -

1.15 match ip route-source

Redistribute routes to destination network routes whose source IP address matches an access list or prefix list rule.

match ip route-source { access-list-number [access-list-number... | access-list-name...] | access-list-name [access-list-number... | access-list-name] | prefix-list prefix-list-name [prefix-list-name...] }

Delete existing configuration.

no match ip route-source [access-list-number [access-list-number... | access-list-name...] | access-list-name [access-list-number... | access-list-name] | prefix-list prefix-list-name [prefix-list-name...]]

【Parameter Description】

Parameter	Description
access-list-number	access list number.
access-list-name	access list name.
prefix-list prefix-list-name	prefix list names to match.

【Default Configuration】-

【Command Mode】 Routing map configuration mode

【Default Level】 14

【Usage Guide】 The match ip route-source command can be followed by multiple access list numbers.

Routing information can be redistributed from one routing process to another routing process. For example, the routes of the OSPF routing domain can be redistributed and advertised to the RIP routing domain, or the routes of the RIP routing domain can be redistributed and advertised to the OSPF routing domain. Mutual redistribution of routes is possible among all IP routing protocols.

In route redistribution, the mutual distribution of routes between two routing domains is often conditionally controlled through the application of route maps. In a routing map rule configuration, one or more match commands and one or more set commands can be executed. If there is no match command, match all; if there is no set command, do nothing.

By default, deleting a configuration without entering a list number will delete all lists.

【Configuration Example]】1: Configure the OSPF routing protocol to redistribute RIP routes. OSPF allows redistribution of RIP routes as long as their routing source IP addresses conform to Access List 5.

```
AC-FS(config)# router ospf
AC-FS(config-router)# redistribute rip subnets AC-FS(config-router)# route-map redrip
AC-FS(config-router)# network 192.168.12.0 0.0.0.255 area 0
AC-FS(config-router)# exit
AC-FS(config)# access-list 5 permit host 192.168.100.1
AC-FS(config)# route-map redrip permit 10 AC-
FS(config-route-map)# match ip route-source 5
```

【Verification】1: Use the show running-config command to view the configuration.

【Prompt Information】-1: If the specified ACL name is invalid (for example, match ip route-source 12345), an error message will be displayed.

```
% ACL name 12345 is invalid
```

2: If the matching prefix-list has been configured before, and then the matching ACL is configured, an error message will be displayed.

```
% Can't set access-list match with prefix-list exits!
```

3: If the matching ACL has been configured before, and the matching prefix-list is configured again, an error message will be displayed.

```
% Can't set prefix-list match with access-list exists!
```

4: If the number of ACLs specified by a single command exceeds 6, an error message will be displayed.

```
% Match ip route-source command only support six IP access-list
```

5: If there are more than 6 ACLs configured in total, an error message will be displayed.

```
% ACL can't exceed 6!
```

6: If the number of prefix-lists specified in a single command exceeds 6, an error message will be displayed.

```
% Match ip route-source command only support six IP prefix-list
```

7: If there are more than 6 prefix-lists configured in total, an error message will be displayed.

```
% Prefix-list can't exceed 6!
```

【Common Mistake】-

【Platform Description】 -

1.16 match length

Configure policy routing based on IP packet length.

match length min-length max-length

delete existing configuration.

no match length min-length max-length

【Parameter Description】

Parameter	Description
min-length	The minimum length of the IP data packet, the value range: 0~65535.
max-length	The maximum length of IP data packets, value range: 0~65535.

【Default Configuration】-

【Command Mode】 Routing map configuration mode

【Default Level】 14

【Usage Guide】 Policy-based routing is a more flexible packet routing and forwarding mechanism than routing based on the target network. When policy routing is applied, the device determines how to process the data packets that need to be routed through the routing map, and the routing map determines the next hop forwarding device for a data packet.

To apply policy routing, you must specify the routing map used by policy routing, and create a routing map. A routing map consists of many policies, each of which defines one or more matching rules and corresponding operations. After policy routing is applied to an interface, all packets received by the interface will be checked. The packets that do not conform to any policy in the routing map will be forwarded according to the usual route, and the packets that conform to a policy in the routing map will be processed according to the routing map. Actions defined in the policy are processed.

If interactive traffic and bulk traffic need to be routed separately, policy routing based on packet size can be used.

【Configuration Example]】1: Enable policy routing on GigabitEthernet 1/0, and send traffic with packets less than 500 bytes from GigabitEthernet 1/2 interface.

```
AC-FS(config)# interface GigabitEthernet 1/0 AC-
FS(config-if)# ip policy route-map smallpak AC-
FS(config-if)# exit
AC-FS(config)# route-map smallpak permit 10
AC-FS(config-route-map)# match length 0 500
AC-FS(config-route-map)# set interface GigabitEthernet 1/2
```

【Verification】1: Use the show running-config command to view the configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】

1.17 match metric

The metric that matches the route.

match metric

Delete matching route metrics.

no match metric

【Parameter Description】

Parameter	Description
metric	Routing metric value, the value range: 0-4294967295.

【Default Configuration】-

【Command Mode】 Routing map configuration mode

【Default Level】 14

[Usage Guide] Routing information can be redistributed from one routing process to another routing process. For example, the routes of the OSPF routing domain can be redistributed and advertised to the RIP routing domain, or the routes of the RIP routing domain can be redistributed and advertised to the OSPF routing domain. Mutual redistribution of routes is possible among all IP routing protocols.
In route redistribution, the mutual distribution of routes between two routing domains is often conditionally controlled through the application of route maps. In a routing map rule configuration, one or more match commands and one or more set commands can be executed. If there is no match command, match all; if there is no set command, do nothing.

【Configuration Example]】 1: OSPF routing protocol redistributes RIP routes. Only RIP routes with a metric value of 10 will be redistributed by OSPF.

```
AC-FS(config)# router ospf
AC-FS(config-router)# redistribute rip subnets route-map redist-rip
AC-FS(config-router)# network 192.168.12.0 0.0.0.255 area 0 AC-
FS(config-router)# exit
AC-FS(config)# route-map redist-rip permit 10
AC-FS(config-route-map)# match metric 10
```

【Verification】1: Use the show running-config command to view the configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.18 match route-type

The route type that matches the route.

match route-type { internal | external [type-1 | type-2] }

Removes matching of route types.

no match route-type [internal | external [type-1 | type-2]]

【Parameter Description】

Parameter	Description
Internal	Internal Routing for OSPF.
external	External Routing (External Routing for OSPF).
type-1 | type-2	Type 1 or Type 2 external routing for OSPF.

【Default Configuration】-

【Command Mode】 Routing map configuration mode

【Default Level】 14

【Usage Guide】Routing information can be redistributed from one routing process to another routing process. For example, the routes of the OSPF routing domain can be redistributed and advertised to the RIP routing domain, or the routes of the RIP routing domain can be redistributed and advertised to the OSPF routing domain. Mutual redistribution of routes is possible among all IP routing protocols.
In route redistribution, the mutual distribution of routes between two routing domains is often conditionally controlled through the application of route maps. In a routing map rule configuration, one or more match commands and one or more set commands can be executed. If there is no match command, match all; if there is no set command, do nothing.

【Configuration Example]】 1: Configure the RIP routing protocol to redistribute OSPF routes. RIP only redistributes the internal routes of the OSPF routing domain.

```
AC-FS(config)# router rip
AC-FS(config-router)# redistribute ospf route-map redrip
AC-FS(config-router)# network 192.168.12.0 AC-FS(config-
router)# exit
AC-FS(config)# route-map redrip permit 10
AC-FS(config-route-map)# match route-type internal
```

【Verification】1: Use the show running-config command to view the configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.19 match tag

The tag to match the route.

match tag tag […tag]

Remove tags matching routes.

no match tag [tag […tag]]

【Parameter Description】

Parameter	Description
tag	The tag value for the route. By default, if the optional Parameter is not entered when deleting the configuration, the tags of all matching routes will be deleted.

【Default Configuration】-

【Command Mode】 Routing map configuration mode

【Default Level】 14

【Usage Guide】 The match tag command can be followed by multiple tags.

Routing information can be redistributed from one routing process to another. For example, the routes of the OSPF routing domain can be redistributed and advertised to the RIP routing domain, or the routes of the RIP routing domain can be redistributed and advertised to the OSPF routing domain. Mutual redistribution of routes is possible among all IP routing protocols.

In route redistribution, the mutual distribution of routes between two routing domains is often conditionally controlled through the application of route maps. In a routing map rule configuration, one or more match commands and one or more set commands can be executed. If there is no match command, match all; if there is no set command, do nothing.

【Configuration Example]】1: Configure the RIP routing protocol to redistribute OSPF routes. RIP only redistributes routes marked 50 and 80 in the OSPF routing domain.

```
AC-FS(config)# router rip
AC-FS(config-router)# redistribute ospf 100 route-map redrip
AC-FS(config-router)# network 192.168.12.0
AC-FS(config-router)#  exit AC-FS(config)#
route-map redrip permit 10
AC-FS(config-route-map)# match tag 50 80
```

【Verification】1: Use the show running-config command to view the configuration.

【Prompt Information】-1: If the total number of configured tags exceeds 4, an error message will be displayed.

```
% Match tag can't exceed 4!
```

【Common Mistake】-

【Platform Description】 -

1.20 memory-lack exit-policy

After the memory reaches the lower line, specify the exit policy of the upper-layer routing protocol.

memory-lack exit-policy { ospf | rip }

Restore default exit policy.

no memory-lack exit-policy

【Parameter Description】

Parameter	Description
ospf	Specify the OSPF protocol to exit first when the memory is insufficient.
rip	Specifies that the RIP protocol will exit first when the memory is insufficient.

【Default Configuration】 Default exit policy: exit the routing protocol with the largest memory usage.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 When the memory reaches the lower line, in order to protect the operation of other protocols in the system, a routing protocol will be closed and the memory resources will be released.

Users should know which routing protocols support the main business of their network, and in the case of insufficient memory, turn off the least important protocol in order to protect the operation of the main business in this extreme situation.

For a routing protocol that is not enabled, specifying a routing protocol to exit first does not help the system to obtain enough memory resources.

This policy is specified only to protect important network services when the system memory is insufficient to a certain extent. If the memory is further consumed, all routing protocols will exit and stop running.

【Configuration Example】Specify the exit policy: RIP exits first

```
AC-FS(config)# memory-lack exit-policy rip
```

【Verification】1: Use the show running-config command to view the configuration.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.21route-map

Define the routing map and enter the routing map configuration mode.

route-map route-map-name [permit | deny] [sequence-number]

Deletes the definition of the specified routing map.

no route-map route-map-name [{ permit | deny } sequence-number]

【Parameter Description】

Parameter	Description
route-map-name	Define a memorable name for the routing map. The routing process redistribution configuration commands refer to the routing map by this name. A routing map can define multiple routing map policies, and a routing map policy corresponds to a sequence number.
permit	If the permit keyword is defined, it conforms to the matching rules defined by match. The set command controls redistribution routing; for policy routing, the set command controls packet forwarding. and exit the routing map operation. If the permit keyword is defined, it does not match the matching rules defined by match. Then it will enter the second route map policy to operate. until the set command is finally executed.
deny	If the deny keyword is defined, it matches the matching rules defined by match. No operation is performed, the route map policy does not allow route redistribution or policy routing, and the route map operation is exited. If the deny keyword is defined, it does not match the matching rules defined by match. Then it will enter the next route map strategy for operation. until the set command is finally executed.
sequence-number	The sequence number corresponding to the routing map policy. Strategies with low sequence numbers are used first, so you need to pay attention to the sequence number settings.

【Default Configuration】 No routing map is configured by default

【**Command Mode**】 Global configuration mode

【**Default Level**】 14

【**Usage Guide**】Currently, the routing graph of RGOS software is mainly used in two places: route redistribution control and policy routing.

Routing redistribution controls how routing information can be redistributed from one routing process to another. For example, the routes of the OSPF routing domain can be redistributed and advertised to the RIP routing domain, or the routes of the RIP routing domain can be redistributed and advertised to the OSPF routing domain. Mutual redistribution of routes is possible among all IP routing protocols.

In route redistribution, the mutual distribution of routes between two routing domains is often conditionally controlled through the application of route maps. In a routing map rule configuration, one or more match commands and one or more set commands can be executed. If there is no match command, match all; if there is no set command, do nothing.

When configuring a routing map, the following points need to be paid attention to when using the routing map sequence number:

1. If the first route map policy is created, sequence-number is not specified, the default is 10;

2. If there is only one routing map policy and no sequence-number is specified, a new routing map policy will not be created, and the existing routing map policy will be directly entered for configuration;

3. If there are multiple routing map policies, the operation must specify the sequence number, otherwise an error message will appear.

【**Configuration Example]**】 1: Configure the OSPF routing protocol to redistribute RIP routes. Only the RIP routes with hops of 4 are required to be redistributed. In the OSPF routing domain, the route type is external route type-1, and the initial metric value is 40. The route tag value is set to 40.

```
AC-FS(config)# router ospf
AC-FS(config-router)# redistribute rip subnets route-map redrip
AC-FS(config-router)# network 192.168.12.0 0.0.0.255 area 0 AC-
FS(config-router)# exit
AC-FS(config)# route-map redrip permit 10 AC-
FS(config-route-map)# match metric 4 AC-
FS(config-route-map)# set metric 40 AC-FS(config-
route-map)# set metric-type type-1
AC-FS(config-route-map)# set tag 40
```

【**Verification**】1: Use the show running-config command to view the configuration.

【**Prompt Information**】-1: If the length of the specified route-map name exceeds 32, an error message will be displayed.

```
% Route-map name string length can not exceed 32.
```

【Common Mistake】-

【Platform Description】 -

1.22 send-lifetime

Configure the lifetime of the keychain sending direction.

send-lifetime start-time { infinite | end-time | duration seconds }

Removes the lifetime for the receive direction of the keychain.

no send-lifetime

【Parameter Description】

Parameter	Description
start-time	Specifies the start time of the lifetime.
infinite	This Parameter indicates that the key is valid from the start time.
end-time	The end time of the key validity period, which must be later than start-time.
duration seconds	Specifies the duration of the validity period starting from start-time, the value range: 1-2147483646.

【Default Configuration】 The keychain sending lifetime is not defined

【Command Mode】 Keychain key configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure keychain kc, enter keychain configuration mode, configure key1, enter key1 configuration mode, and define keychain reception lifetime

```
AC-FS(config)#key chain kc AC-
FS(config-keychain)#key 1
AC-FS(config-keychain-key)#key-string World
AC-FS(config-keychain-key)#send-lifetime 16:30:00 Oct 1 2010 duration 43200
```

【Verification】1: Use the show running-config command to view the configuration.

【Common Mistake】-

【Platform Description】 -

1.23 set default interface

Specifies the default forwarding interface for packets that match the match rule and do not have an explicit egress route.

set default interface interface-type interface-number […interface-type interface-number]

Delete the set default forwarding interface.

no set default interface interface-type interface-number […interface-type interface-number]

【Parameter Description】

Parameter	Description
interface-type	Interface Type.
interface-number	interface Code.

【Default Configuration】-

【Command Mode】 Routing map configuration mode

【Default Level】 14

【Usage Guide】 The set default interface command can be followed by multiple interfaces.

Policy-based routing is a more flexible packet routing and forwarding mechanism than routing based on the target network. When policy routing is applied, the device will determine how to process the data packets that need to be routed through the routing map, and the routing map determines the next hop forwarding device for a data packet.

To apply policy routing, you must specify the routing map used by policy routing, and create a routing map. A routing map consists of many policies, each of which defines one or more matching rules and corresponding operations. After policy routing is applied to an interface, all packets received by the interface will be checked. The packets that do not conform to any policy in the routing map will be forwarded according to the usual route, and the packets that conform to a policy in the routing map will be processed according to the routing map. Actions defined in the policy are processed.

If the state of the first defined interface goes down, the interface set by the second set command will be tried. There can be multiple sets in a route map policy operate.

【Configuration Example]】1: Enable policy routing on serial 1/0. When the interface receives traffic with packets less than 500 bytes and there is no clear route in the routing table, it will send packets from the GigabitEthernet 1/0 interface.

```
AC-FS(config)# interface serial 1/0 AC-
FS(config-if)# ip policy route-map smallpak AC-
FS(config-if)# exit
AC-FS(config)# route-map smallpak permit 10
AC-FS(config-route-map)# match length 0 500
AC-FS(config-route-map)# set default interface GigabitEthernet 1/0
```

【Verification】1: Use the show running-config command to view the configuration.

【Prompt Information】 1: If set vrf has been configured before, an error message will be displayed.

```
% Route-map: can not set default interface.
% Remove set vrf clause before set default interface.
```

2: If the number of specified interfaces exceeds 4, an error message will be displayed.

```
% Set default interface can't exceed 4!
```

3: If the specified interface is a Layer 2 port (such as Layer 2 port GigabitEthernet 0/0), an error message will be displayed.

```
% Invalid parameter: GigabitEthernet 0/0, only support layer 3 interface.
```

【Common Mistake】-

【Platform Description】 -

1.24set interface

Specify the forwarding interface for packets matching the match rule.

set interface interface-type interface-number […interface-type interface-number]

Delete the configuration that sets the forwarding interface.

no set interface interface-type interface-number […interface-type interface-number]

【Parameter Description】

Parameter	Description
interface-type	Interface Type.
interface-number	interface Number.

【Default Configuration】-

【Command Mode】 Routing map configuration mode

【Default Level】 14

【Usage Guide】 Multiple interfaces can be configured after the set interface command.

Policy-based routing is a more flexible packet routing and forwarding mechanism than routing based on the target network. When policy routing is applied, the device will determine how to process the data packets that need to be routed through the routing map, and the routing map determines the next hop forwarding device for a data packet.

To apply policy routing, you must specify the routing map used by policy routing, and create a routing map. A routing map consists of many policies, each of which defines one or more matching rules and corresponding operations. After policy routing is applied to an interface, all packets received by the interface will be checked. The packets that do not conform to any policy in the routing map will be forwarded according to the usual route, and the packets that conform to a policy in the routing map will be processed according to the routing map. Actions defined in the policy are processed.

If the state of the first defined interface goes down, the interface set by the second set command will be tried. There can be multiple set operations in a routemap policy.

If the interface is set to null 0, the packet will be dropped.

【Configuration Example]】1: Enable policy routing on serial 1/0, and send packets less than 500 bytes received on the interface from the GigabitEthernet 0/0 interface.

```
AC-FS(config)#interface serial 1/0 AC-
FS(config-if)#ip policy route-map smallpak AC-
FS(config)#route-map smallpak permit 10 AC-
FS(config-route-map)#match length 0 500
AC-FS(config-route-map)#set interface GigabitEthernet 0/0
```

【Verification】1: Use the show running-config command to view the configuration.

【Prompt Information】 1: If set vrf has been configured before, an error message will be displayed.

```
% Route-map: can not set interface.

% Remove set vrf clause before set interface.
```

2: If the number of specified interfaces exceeds 4, an error message will be displayed.

```
% Set interface can't exceed 4!
```

3: If the specified interface is a Layer 2 port (such as Layer 2 port GigabitEthernet 0/0), an error message will be displayed.

```
% Invalid parameter: GigabitEthernet 0/0, only support layer 3 interface.
```

【Common Mistake】-

【Platform Description】 -

1.25set ip default next-hop

Specifies the default next-hop IP address for packets matching the match rule.

set ip [global] default next-hop ip-address [weight] […ip-address [weight]]

Delete the configuration that sets the default next hop.

no set ip [vrf vrf-name | global] default next-hop [ip-address [weight] […ip-address [weight]]]

【Parameter Description】

Parameter	Description
vrf vrf-name	The next hop address belongs to the specified VRF. If a multiprotocol VRF is specified, the VRF must first activate the IPv4 address family.
global	The next hop address belongs to the global.
ip-address	The next hop IP address.
weight	The weight of the current next hop.

【Default Configuration】-

【Command Mode】 Routing map configuration mode

【Default Level】 14

【Usage Guide】 This set command has two operation modes: WCMP load balancing operation mode and non-WCMP load balancing operation mode. In the former operating mode, the system will perform WCMP load balancing on the traffic according to the weight value input by the user.

The set ip default next-hop command can be followed by multiple IP addresses, up to a maximum of 32.

If the weight value is added after the ip address, no more than 4 nexthop addresses can be configured.

If the Parameter "vrf vrf-name" is specified, the packet will be forwarded across the VRF; if the Parameter "global" is specified, the packet will be forwarded from the VRF to the public network; if the Parameter "[vrf vrf-name | global]" is not specified , the VRF will be inherited when the packet is forwarded, that is, the next hop belongs to the VRF that receives the packet.

Any next-hop followed by the weight value will automatically switch the operation mode of this set command to the WCMP load balancing operation mode. In WCMP load balancing operation mode, for those nexthop addresses that are not configured with corresponding weights, their weights default to 1.

The difference between the set ip next-hop and set ip default next-hop commands is that: the system configured with the set ip next-hop command preferentially uses policy routing when forwarding packets; the system configured with set ip default next-hop will forward packets. The routing and forwarding table is preferentially used when writing.

Use this command to provide the ability to set a custom default route for a specific user. If the software cannot find a forwarding route for the packet to be forwarded, the packet is forwarded to the next hop configured by this command.

To apply policy routing, you must specify the routing map used by policy routing, and create a routing map. A routing map consists of many policies, each of which defines one or more matching rules and corresponding operations. After policy routing is applied to an interface, all packets received by the interface will be checked. The packets that do not conform to any policy in the routing map will be forwarded according to the usual route, and the packets that conform to a policy in the routing map will be processed according to the routing map. Actions defined in the policy are processed.

There can be multiple set operations in a routemap policy.

【Configuration Example]】 1: The packets sent from 1.1.1.1 received on synchronous interface 1 will be forwarded to device 6.6.6.6 if the software cannot find the forwarding route; And the received message from 2.2.2.2 will be forwarded to device 7.7.7.7 if the software cannot find the forwarding route. Other packets are discarded if the software cannot find a forwarding route.

```
AC-FS(config)#access-list 1 permit 1.1.1.1 0.0.0.0
```

```
AC-FS(config)#access-list 2 permit 2.2.2.2 0.0.0.0 AC-
FS(config)#interface async 1
AC-FS(config-if)#ip policy route-map equal-access AC-
FS(config)#route-map equal-access permit 10 AC-FS(config-
route-map)#match ip address 1 AC-FS(config-route-map)#set
ip default next-hop 6.6.6.6 AC-FS(config)#route-map
equal-access permit 20 AC-FS(config-route-map)#match ip
address 2 AC-FS(config-route-map)#set ip default next-hop
7.7.7.7 AC-FS(config)#route-map equal-access permit 30
AC-FS(config- route-map)#set default interface null 0
```

【Verification】1: Use the show running-config command to view the configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.26 set ip dscp

Set the DSCP value for the packets matching the match rule.

set ip dscp dscp_value

Remove the set DSCP value.

no set ip dscp

【Parameter Description】

Parameter	Description
dscp_value	Set the DSCP value of the IP header in the IP packet.

【Default Configuration】-

【Command Mode】 Routing map configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】-

【Verification】1: Use the show running-config command to view the configuration.

【Prompt Information】 1: If set ip tos/precedence has been configured before, an error message will be displayed.

```
% Route-map: can not set ip dscp.
% Remove set ip tos/precedence clause before set ip dscp.
```

【Common Mistake】-

【Platform Description】 -

1.27set ip next-hop

Specifies the next-hop IP address for packets matching the match rule.

set ip [vrf vrf-name | global] next-hop ip-address [weight] […ip-address [weight]]

Delete set next hop IP.

no set ip [vrf vrf-name | global] next-hop [ip-address [weight] […ip-address [weight]]]

【Parameter Description】

Parameter	Description
vrf vrf-name	The next hop address belongs to the specified VRF. If a multiprotocol VRF is specified, the VRF must first activate the IPv4 address family.
global	The next hop address belongs to the global.
ip-address	The next hop IP address.
weight	The weight of the current next hop.

【Default Configuration】-

【Command Mode】 Routing map configuration mode

【Default Level】 14

【Usage Guide】 This command is only used for policy routing configuration.

This set command has two operation modes: WCMP load balancing operation mode and non-WCMP load balancing operation mode. In the former operating mode, the system will perform WCMP load balancing on the traffic according to the weight value entered by the user.

The set ip next-hop command can be followed by multiple IP addresses, up to a maximum of 32.

If the weight value is added after the ip address, no more than 4 nexthop addresses can be configured.

If the Parameter "vrf vrf-name" is specified, the packet will be forwarded across the VRF; if the Parameter "global" is specified, the packet will be forwarded from the VRF to the public network; if the Parameter "[vrf vrf-name | global]" is not specified , the VRF will be inherited when the packet is forwarded, that is, the next hop belongs to the VRF that receives the packet.

Any next-hop followed by the weight value will automatically switch the operation mode of this set command to the WCMP load balancing operation mode. In the WCMP load balancing mode, for the nexthop addresses that do not have the corresponding weight configured, the default weight is 1.

Policy routing is a more flexible packet routing and forwarding mechanism than routing based on the target network. When policy routing is applied, the device determines how to process the data packets that need to be routed through the routing map, and the routing map determines the next hop forwarding device for a data packet.

To apply policy routing, you must specify the routing map used by policy routing, and create a routing map. A routing map consists of many policies, each of which defines one or more matching rules and corresponding operations. After policy routing is applied to an interface, all packets received by the interface will be checked. The packets that do not conform to any policy in the routing map will be forwarded according to the usual route, and the packets that conform to a policy in the routing map will be processed according to the routing map. Actions defined in the policy are processed.

There can be multiple set operations in a routemap policy.

【Configuration Example]】 1: Enable policy routing on serial 1/0. If an interface receives a packet with a source address in the 10.0.0.0/8 range, it will be sent to 192.168.100.1; traffic with a source network in the 172.16.0.0/16 range will be sent to 172.16.100.1; the rest All data traffic will be dropped.

```
AC-FS(config)#interface serial 1/0
AC-FS(config-if)#ip policy route-map load-balance AC-
FS(config)#access-list 10 permit 10.0.0.0 0.255.255.255 AC-
FS(config)#access-list 20 permit 172.16.0.0 0.0.255.255 AC-
FS(config)#route-map load-balance permit 10 AC-FS(config-
route-map)#match ip address 10
AC-FS(config-route-map)#set ip next-hop 192.168.100.1
AC-FS(config)#route-map load-balance permit 20 AC-
FS(config-route-map)#match ip address 20 AC-FS(config-
route-map)#set ip next-hop 172.16.100.1 AC-
FS(config)#route-map load-balance permit 30
AC-FS(config-route-map)#set interface Null 0
```

【Verification】 1: Use the show running-config command to view the configuration.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.28 set ip next-hop verify-availability

Specifies to confirm the reachability of the next-hop IP address.

set ip next-hop verify-availability ip-address

Delete existing configuration.

no set ip next-hop verify-availability ip-address

【Parameter Description】

Parameter	Description
ip-address	next hop IP address.

【Default Configuration】 -

【Command Mode】 Routing map configuration mode

【Default Level】 14

【Usage Guide】 This command is only used for policy routing configuration.

【Configuration Example】-

【Verification】 1: Use the show running-config command to view the configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.29set ip precedence

Set the priority of the IP header for the packets matching the match rule.

set ip precedence { number | critical | flash | flash-override | immediate | internet | network | priority | routine }

Remove the configuration that sets the priority of the IP header.

no set ip precedence

【Parameter Description】

Parameter	Description
number	A number that indicates the priority of the IP header. The value range is 0-7. 7: critical 6: flash 5: flash-override 4: immediate 3: internet 2: network

	1: priority 0: routine
critical | flash | flash-override | immediate | internet | network | priority | routine	The priority of the P header.

【Default Configuration】-

【Command Mode】 Routing map configuration mode

【Default Level】 14

【Usage Guide】 The priority value in the IP packet header is often set to make the IP packets routed by the policy route to be transmitted with different priorities.

In the routing map configuration rule, you can configure multiple set ip precedence commands, but only the last one is valid, and as long as the IP header of the packet matches the policy route, the specified priority will be set.

【Configuration Example]】1: Set precedence to 4 for packets with source address 192.168.217.68 coming from interface GigabitEthernet 0/0.

```
AC-FS(config)#access-list 1 permit 192.168.217.68 0.0.0.0
AC-FS(config)#route-map name
AC-FS(config-route-map)#match ip address 1
AC-FS(config-route-map)#set ip precedence 4
AC-FS(config)#interface GigabitEthernet 0/0
AC-FS(config-if)#ip policy route-map name
```

【Verification】1: Use the show running-config command to view the configuration.

【Prompt Information】 1: If set ip dscp has been configured before, an error message will be displayed.

【Common Mistake】-

【Platform Description】 -

1.30set ip tos

Set the TOS of the IP header of the packet for the packet matching the match rule.

set ip tos { number | max-reliability | max-throughput | min-delay | min-monetary-cost | normal }

Delete existing configuration.

no set ip tos

【Parameter Description】

Parameter	Description
number	Indicates the TOS of the IP header as a number. The value range is 0-15.
max-reliability | max-throughput | min-delay | min-monetary-cost | normal	The priority of the IP header. Correspondence with numbers: max-reliability: 2 max-throughput: 4 min-delay: 8 min-monetary-cost: 1 normal: 0

【Default Configuration】-

【Command Mode】 Routing map configuration mode

【Default Level】 14

【Usage Guide】IP packets using policy routing are often transmitted with different quality of service by setting the TOS value in the IP packet header. As long as the IP header of the packet matching the policy route will be set to the specified TOS value.

【Configuration Example]】 1: Set tos to 4 for packets with source address 192.168.217.68 coming from interface GigabitEthernet 0/0.

```
AC-FS(config)#access-list 1 permit 192.168.217.68 0.0.0.0
AC-FS(config)#route-map name
AC-FS(config-route-map)#match ip address 1
AC-FS(config-route-map)#set ip tos 4 AC-
FS(config)#interface GigabitEthernet 0/0
AC-FS(config-if)#ip policy route-map name
```

【Verification】 1: Use the show running-config command to view the configuration.

【Prompt Information】 1: If set ip dscp has been configured before, an error message will be displayed.

```
% Route-map: can not set ip tos.
% Remove set ip dscp clause before set ip tos.
```

【Common Mistake】 -

【Platform Description】 -

1.31set level

Indicates the type of target area to import for routes matching the match rule.

set level { stub-area | backbone }

Delete existing configuration.

no set level

【Parameter Description】

Parameter	Description
stub-area	Specifies to redistribute route advertisements to the OSPF Stub Area.
backbone	Specifies to redistribute route advertisements to the OSPF backbone.

【Default Configuration】 -

【Command Mode】 Routing map configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: The OSPF routing protocol redistributes RIP routes to the backbone area.

```
AC-FS(config)# router ospf
AC-FS(config-router)# redistribute rip subnets route-map redrip
AC-FS(config-router)# network 192.168.12.0 0.0.0.255 area 0 AC-
FS(config-router)# exit
AC-FS(config)# route-map redrip permit 10
AC-FS(config-route-map)# set level backbone
```

【Verification】1: Use the show running-config command to view the configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.32set metric

Set a metric for routes that match the match rule.

set metric [+ metric-value | - metric-value | metric-value]

Delete existing configuration.

no set metric

【Parameter Description】

Parameter	Description
+	Increase (increase on the metric of the original route).
-	Decrease (decrease on the metric of the original route).
metric-value	Set the metric for redistribution routes, the value range: 0-4294967295.

【Default Configuration】-

【Command Mode】 Routing map configuration mode

【Default Level】 14

【Usage Guide】 The route metric value will affect the route selection, so it needs to be set carefully according to the actual network topology. When performing set metric and '+' or '-' metric operations, you should pay attention to the upper and lower limits of each routing protocol. For example, when redistributing other protocol routes for the RIP protocol, the range of the result after the metric is increased or decreased is 1-16.

Routing information can be redistributed from one routing process to another routing process. For example, the routes of the OSPF routing domain can be redistributed and advertised to the RIP routing domain, or the routes of the RIP routing domain can be redistributed and advertised to the OSPF routing domain. Mutual redistribution of routes is possible among all IP routing protocols.

In route redistribution, the mutual distribution of routes between two routing domains is often conditionally controlled through the application of route maps. In a routing map rule configuration, one or more match commands and one or more set commands can be executed. If there is no match command, match all; if there is no set command, do nothing.

【Configuration Example]】1: Configure the OSPF routing protocol to redistribute RIP routes, and set the initial metric value of the redistributed routes to 40.

```
AC-FS(config)# router ospf
AC-FS(config-router)# redistribute rip subnets route-map redrip
AC-FS(config-router)# network 192.168.12.0 0.0.0.255 area 0
AC-FS(config-router)# exit
```

```
AC-FS(config)# route-map redrip permit 10
AC-FS(config-route-map)# set metric 40
```

【Verification】1: Use the show running-config command to view the configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.33set metric-type

Sets the metric type for routes that match the match rule.

set metric-type type

Remove set route metric type.

no set metric-type

【Parameter Description】

Parameter	Description
type	Sets the type of redistribution route. The default type of OSPF redistributed routes is type-2.

【Default Configuration】-

【Command Mode】 Routing map configuration mode

【Default Level】 14

【Usage Guide】Routing information can be redistributed from one routing process to another routing process. For example, the routes of the OSPF routing domain can be redistributed and advertised to the RIP routing domain, or the routes of the RIP routing domain can be redistributed and advertised to the OSPF routing domain. Mutual redistribution of routes is possible among all IP routing protocols.
In route redistribution, the mutual distribution of routes between two routing domains is often conditionally controlled through the application of route maps. In a routing map rule configuration, one or more match commands and one or more set commands can be executed. If there is no match command, match all; if there is no set command, do nothing.

【Configuration Example]】1: Configure the OSPF routing protocol to redistribute RIP routes, and set the redistribution route type to type-1.

```
AC-FS(config)# router ospf
AC-FS(config-router)# redistribute rip subnets route-map redrip
AC-FS(config-router)# network 192.168.12.0 0.0.0.255 area 0
AC-FS(config-router)# exit
```

```
AC-FS(config)# route-map redrip permit 10
AC-FS(config-route-map)# set metric-type type-1
```

【Verification】1: Use the show running-config command to view the configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.34set next-hop

Specify the next-hop IP address for routing information matching the match rule.

set next-hop ip-address

Delete the set route next hop.

no set next-hop

【Parameter Description】

Parameter	Description
ip-address	next hop IP address.

【Default Configuration】-

【Command Mode】 Routing map configuration mode

【Default Level】 14

【Usage Guide】 This command is only used for routing policy configuration.

Routing information can be redistributed from one routing process to another routing process. For example, the routes of the OSPF routing domain can be redistributed and advertised to the RIP routing domain, or the routes of the RIP routing domain can be redistributed and advertised to the OSPF routing domain. Mutual redistribution of routes is possible among all IP routing protocols. In route redistribution, the mutual distribution of routes between two routing domains is often conditionally controlled through the application of route maps. In a routing map rule configuration, one or more match commands and one or more set commands can be executed. If there is no match command, match all; if there is no set command, do nothing.

【Configuration Example]】1: Set the next hop of the route matching ACL 1 to 192.168.1.2.

```
AC-FS(config)# route-map redrip permit 10
AC-FS(config-route-map)# match ip address 1 AC-
FS(config-route-map)# set next-hop 192.168.1.2
AC-FS(config)# route-map redrip permit 10
AC-FS(config-route-map)# match ip address 1 AC-
FS(config-route-map)# set next-hop 192.168.1.2
```

【Verification】1: Use the show running-config command to view the configuration.

【Prompt Information】 1: If the configured IP address is not a valid host address (effectively including A class divided by 0 and beginning with 127, B class and C class), an error message will be prompted.

% Can't set invalid nexthop address!

【Common Mistake】 -

【Platform Description】 -

1.35set tag

Set a flag on routes that match the match rule.

set tag tag

Remove the set route flag.

no set tag

【Parameter Description】

Parameter	Description
tag	Set the flag of the redistribution route, the value range: 0-4294967295.

【Default Configuration】-

【Command Mode】 Routing map configuration mode

【Default Level】 14

【Usage Guide】 This command is valid only for route redistribution. If this command is not configured, the original routing tag will be inherited.

【Configuration Example]】1: Configure the OSPF routing protocol to redistribute RIP routes, and set the flag of the redistributed route to 100.

```
AC-FS(config)# router ospf
AC-FS(config-router)# redistribute rip subnets route-map redrip
AC-FS(config-router)# network 192.168.12.0 0.0.0.255 area 0 AC-
FS(config-router)# exit
AC-FS(config)# route-map redrip permit 10
AC-FS(config-route-map)# set tag 100
```

【Verification】1: Use the show running-config command to view the configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.36 show ip as-path-access-list

Displays information about the community list.

show ip as-path-access-list [num]

【Parameter Description】

Parameter	Description
num	as-path-access-list number.

【Command Mode】Privileged mode, global configuration mode, interface configuration mode, routing protocol configuration mode, routing map configuration mode, etc.

【Default Level】 14

【Usage Guide】 Use this command to view the information of as-path-access-list.

【Configuration Example】1: Display the AS path list.

```
AC-FS# show ip as-path-access-list
AS path access list 30
permit ^30$
```

Field Description:

Field	Description
AS path access list	The name of the AS path list.
permit	The pattern of the filter rule.
^30$	Specific regular expression rules.

【Prompt Information】 -

【Platform Description】 -

1.37 show ip community-list

Displays information about the community list.

show ip community-list [community-list-number | community-list-name]

【Parameter Description】

Parameter	Description
community-list-number	The community list number for which information is to be displayed. List of Standard Groups: Numbers in the range 1-99 Extended community list: numbering range 100-199
community-list-name	The name of the community list for which to display information. The community list name cannot exceed 80 characters.

【Command Mode】Privileged mode, global configuration mode, interface configuration mode, routing protocol configuration mode, routing map configuration mode, etc.

【Default Level】 14

【Usage Guide】 Use this command to view the information of the community list.

【Configuration Example】1: Display the list of community attributes.

```
AC-FS# show ip community-list
Community-list standard local
permit local-AS
Community-list standard Red-Giant
permit 0:10
deny 0:20
```

Field Description:

Field	Description
Community-list standard local	The type and name of the community attribute list.
permit	The pattern of the filter rule.

local-AS	Community attribute value.
0:10	Community attribute value.

【Prompt Information】-

【Platform Description】 -

1.38 show ip extcommunity-list

Displays configuration information for the extended community attribute list.

show ip extcommunity-list [extcommunity-list-num | extcommunity-list-name]

【Parameter Description】

Parameter	Description
extcommunity-list-num	The value range is [1~199], and the numerical id is used to identify the standard (or extended) extcommunity list.
extcommunity-list-name	the name of the standard (or extended) extcommunity list

【Command Mode】Privileged mode, global configuration mode, interface configuration mode, routing protocol configuration mode, routing map configuration mode, etc.

【Default Level】 14

【Usage Guide】-

【Configuration Example】 1: Display the list of extended community attributes.

```
AC-FS # show ip extcommunity-list
Standard extended community-list 1
     10 permit RT:1:200
     20 permit RT:1:100
Standard extended community-list 2
     10 permit RT:1:200
Expanded extended community-list rt_filter
     13 permit 1:100
```

Field Description:

Field	Description
Standard extended community-list 1	The type and name of the extended community attribute list.
10	The sequence number of the filter rule.
permit	The pattern of the filter rule.
RT:1:200	Extended community attribute value.

【Prompt Information】-

【Platform Description】 -

【Prompt Information】-

【Platform Description】 -

1.39 show ip prefix-list

View prefix list information or prefix list entry information.

show ip prefix-list [prefix-name]

【Parameter Description】

Parameter	Description
prefix-name	prefix list name.

【Command Mode】Privileged user mode, global configuration mode, interface configuration mode, routing protocol configuration mode, routing map configuration mode, etc.

【Default Level】 14

【Usage Guide】If no prefix list name is specified, the configuration information of all prefix lists will be displayed, otherwise only the configuration information of the specified prefix list will be displayed.

【Configuration Example】1: Display the IPv4 prefix list.

```
AC-FS# show  ip  prefix-list
ip prefix-list pre: 2 entries
seq 5 permit 192.168.64.0/24
seq 10 permit 192.2.2.0/24
```

Field Description:

Field	Description
ip prefix-list pre	IPv4 prefix list name.
2 entries	The number of rules the prefix list contains.
seq 5	The sequence number of the filter rule.
permit	The pattern of the filter rule.
192.168.64.0/24	IPv4 routing prefix.

【Prompt Information】-

【Platform Description】 -

1.40 show ip protocols

View the status information of currently running IPv4 routing protocols.

show ip protocols {ospf | rip }

【Parameter Description】

Parameter	Description
ospf	Displays OSPF protocol status information.
rip	Displays RIP protocol status information.

-	Displays status information for all running routing protocols.

【Command Mode】 Privileged user mode, global configuration mode, interface configuration mode, routing protocol configuration mode, routing map configuration mode, etc.

【Default Level】 14

【Usage Guide】 Only the status information of the currently running routing protocol is displayed, and the routing protocol that is not enabled will not be displayed.

【Configuration Example】 1: Display routing protocol status

```
AC-FS# show ip protocols
Routing Protocol is "ospf 1"
```

```
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 57.57.57.57
  Memory Overflow is enabled
  Router is not in overflow state now
  It is an autonomous system boundary router
  Redistributing External Routes from,
    connected, includes subnets in redistribution
    bgp, includes subnets in redistribution
  Number of areas in this router is 2: 2 normal 0 stub 0 nssa
  Routing for Networks:
    57.57.57.57 0.0.0.0 area 0
    163.18.4.0 0.0.0.255 area 0
    163.18.57.0 0.0.0.255 area 0
    192.100.1.0 0.0.0.255 area 0
    192.101.1.0 0.0.0.255 area 1
    192.102.1.0 0.0.0.255 area 0
  Reference bandwidth unit is 100 mbps
  Distance: (default is 110)

Routing Protocol is "bgp 10"
  IGP synchronization is disabled
  Default-information originate is disabled
  Default local-preference applied to incoming route is 100
  Redistributing: connected
  Neighbor(s):
    Address          AddressFamily FiltIn FiltOut DistIn  DistOut  RouteMapIn  RouteMapOut
Weight
  Distance: external 20(default) internal 200(default) local 200(default)
```

Field Description：

Field	Description
Routing Protocol is "ospf 1"	the name of the routing protocol.
Redistributing External Routes from	Redistribution routing state of routing protocols.
Di tance:	Distance information of routing protocols.

【Prompt Information】-

【Platform Description】 -

1.41 show key chain

Displays configuration information for the keychain.

show key chain [keychain name]

【Parameter Description】

Parameter	Description
keychain name	Only display configuration information for the specified keychain.

【Command Mode】Privileged user mode, global configuration mode, interface configuration mode, routing protocol configuration mode, routing map configuration mode, etc.

【Default Level】 14

【Usage Guide】If the keychain name is not specified, the configuration information of all keychains will be displayed, otherwise only the configuration information of the specified keychain will be displayed.

【Configuration Example】1: Display the keychain.

```
AC-FS# show key chain
route-map AAA, permit, sequence 10
Match clauses:
ip address 2
Set clauses:
metric 10
AC-FS(config)#show key chain
key chain kc
    key 1 -- text "AC-FS"
        accept-lifetime (12:11:00 May  2 2001) - (infinite)
        send-lifetime (always valid) - (always valid) [valid now]
```

Field Description:

Field	Description
key chain	keychain name.
key	key id and key string.
accept-lifetime	The lifetime of the keychain receiving direction.

send-lifetime	The lifetime of the keychain sending direction.

【Prompt Information】-

【Platform Description】 -

1.42 show route-map

Displays the configuration information of the routing map.

show route-map [route-map-name]

【Parameter Description】

Parameter	Description
route-map-name	Only display the configuration information of the specified routing map.

【Command Mode】Privileged user mode, global configuration mode, interface configuration mode, routing protocol configuration mode, routing map configuration mode, etc.

【Default Level】 14

【Usage Guide】If no routing map name is specified, the configuration information of all routing maps will be displayed, otherwise only the configuration information of the specified routing map will be displayed.

【Configuration Example]】1: Display the routing map.

```
AC-FS# show route-map
route-map AAA, permit, sequence 10
Match clauses:
ip address 2
Set clauses:
metric 10
```

Field Description:

Field	Description
route-map	route map name.
Permit	The route map policy contains the permit keyword.
sequence 10	The sequence number corresponding to the routing map

	policy.
Match clauses	Define matching rules. Determine whether to perform the set operation according to whether the route map policy is the permit or deny keyword.
Set claus s	Define the action after matching the match matching rule.

【Prompt Information】-

【Platform Description】 -

2 NSM

2.1 clear ip route

To clear the routing table cache, execute the clear ip route command in privileged user mode.

clear ip route { * | network [netmask] | }

【Parameter Description】

Parameter	Description
*	Clear all route caches.
network	The network or subnet address to clear cache.
netmask	(Optional) Network mask, if no mask is specified, it means to use the longest matching route in the network routing table and clear the cache.

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】 Clearing the route cache will delete the corresponding route, and then trigger the re-learning of the routing protocol. It must be noted that if the cache of the entire routing table is cleared, it will cause a brief communication interruption of the entire network.

【Configuration Example]】Clear the cache of the longest matching routing table entry of 192.168.12.0.

clear ip route 192.168.12.0

【Prompt Information】-

【Platform Description】 -

2.2ip default-network

Configure the default network.

ip default-network network

Delete the default network.

no ip default-network network

Restore Default Configuration

default ip default-network network

【Parameter Description】

Parameter	Description
network	The network number of the default network.

【Default Configuration】 The default is 0.0.0.0/0.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】 The purpose of configuring a default network is to generate a default route. To generate a default route through default-network, the following conditions must be met: The default network is not a directly connected interface network, but can be reached in the routing table.

The default network always begins with a "*" sign, indicating that it is a candidate for the default route. If there are connected routes and routes without next hops in the default network, the default route is required to be a static route.

【Configuration Example]】 1: Set the 192.168.100.0 network as the default network. Since a static route to this network is configured, the device will automatically generate a default route.

```
AC-FS(config)# ip route 192.168.100.0 255.255.255.0 serial  0/1
AC-FS(config)# ip default-network 192.168.100.0
```

2: Set the 200.200.200.0 network as the default network, as long as 200.200.200.0 appears in the routing table, this route becomes the default route.

```
AC-FS(config)# ip default-network 200.200.200.0
```

【Verification】 You can use show ip route to view the default route.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

2.3ip route

Configure static routes.

ip route network net-mask { ip-address | interface [ip-address] } [distance] [tag tag] [permanent] [weight number] [description description-text] [disabled | enabled] [global]

Delete the configured static route.

no ip route network net-mask { ip-address | interface [ip-address] } [distance]

Delete all configured static routes.

no ip route all

Restore Default Configuration.

default ip route network net-mask { ip-address | interface [ip-address] } [distance]

default ip route all

【Parameter Description】

Parameter	Description
network	The network address of the destination network.
net-mask	target network mask.
ip-address	(Optional) The next hop address of the static route. At least one of ip-address and interface must be specified, or both. When no ip-address is specified, it means to configure a static direct route.
interface	(Optional) The next-hop egress of the static route. At least one of ip-address and interface must be specified, or both. When interface is not specified, it means that a static recursive route is configured, and the egress is obtained by selecting a route in the routing table by the next hop.
distance	(Optional) Administrative distance of static routes, the default is 1.
tag	(Optional) The tag value of the static route. The default value is 0.
permanent	(Optional) Permanent route identifier, the default is non-permanent route.
weight number	(Optional) The weight of the static route. The default value is 1.
description description-text	（Optional) Static route Description information, no Description information by default, description-text is a string of 1 to 60 characters.
disabled/enabled	(Optional) The enable flag of static routing, the default is enabled.

global	(Optional) Displays that the specified next hop belongs to the global routing table, and the default next hop also belongs to the global routing table.

【Default Configuration】 No static route.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】 The default administrative distance of a static route is 1. By setting the administrative distance, the route learned by the dynamic route can be allowed to overwrite the static route. Only when the dynamic route cannot be learned, the static route is used. By setting the administrative distance of the static route, you can realize the backup of the line. The static route at this time is generally called the floating route. For example, the administrative distance of the OSPF routing protocol is 110, and the administrative distance of the static route can be set to 125, so that when the line running OSPF fails, the data traffic can naturally be switched to the line of the static route.

The default weight of static routes is 1. You can use the show ip route weight command to view static routes with non-default weights. Weight Parameterweight is used to implement the WCMP function. When there is a load balancing route that can reach a certain address, the network device will allocate data traffic according to the weight value of each route. The route with a larger weight will share more data packets, and the smaller Fewer data packets will be shared.

The enable flag of the static route controls whether the static route is valid. If it is invalid, it will not be used for forwarding. The permanent route is configured in the forwarding table, and will always exist unless it is deleted through the network management.

When configuring a static route through an Ethernet interface, try to avoid the next hop being an interface directly (eg ip route 0.0.0.0 0.0.0.0 GigabitEthernet 0/0). This will make the device think that all unknown target networks are directly connected to the GigabitEthernet 0/0 interface, so sending an ARP request to each target host will take up a lot of CPU and memory resources. Therefore, it is generally not recommended to point the static route directly to the Ethernet interface.

【Configuration Example]】 1: Add a static route to the 172.16.100.0/24 destination network, the next hop is 192.168.12.1, and the administrative distance is 115.

```
ip route 172.16.100.0 255.255.255.0 192.168.12.1 115
```

2: If the static route does not specify an interface, when the normal sending interface fails, data traffic may be sent from other interfaces. To avoid this situation, you need to specify the interface. In the following configuration example, data traffic to the destination network 172.16.100.0/24 can only be forwarded from the GigabitEthernet 0/0 interface.

```
AC-FS(config)# ip route 172.16.100.0 255.255.255.0 GigabitEthernet 0/0 192.168.12.1
```

【Verification】 You can use show ip route to view the routing table.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.4ip routing

Enables the IP routing feature of the RGOS software.

ip routing

Disable IP routing.

no ip routing

Restore Default Configuration

default ip routing

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 Enable IP routing.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】When the device only acts as a bridge device or only as a VOIP gateway device, the IP routing and forwarding function of the FSOS software may not be needed. At this time, the IP routing function of RGOS can be disabled.

After the IP routing function is disabled, the device behaves like a normal host, and can send and receive packets locally, but cannot forward. All routing related configurations are removed. Static routing configuration is an exception. Since there may be many static routing configurations, if users configure no ip routing inadvertently, a large number of static routing configurations may be lost. To avoid this situation, when no ip routing is executed, the static routing configuration will be temporarily hidden. If the user executes ip routing again, the static routing configuration can be restored.

Note that if the process restarts or the entire system restarts in the case of no ip routing, the static routing configuration will not be retained.

【Configuration Example]】 Disable the IP routing function of the FSOS software.

```
AC-FS(config)# no ip routing
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.5ip static route-limit

Configure the maximum number of static routes.

ip static route-limit number

Configure the default number of routes.

no ip static route-limit

Restore Default Configuration.

default ip static route-limit

【Parameter Description】

Parameter	Description
number	Routing cap, range 1-10000.

【Default Configuration】 The default value is 1024.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】 The purpose of configuring the upper limit of the number of static routes is to control the number of static routes. After configuring the upper limit of the number of static routes through ip static route-limit, the following effects will be produced. The number

of configured static routes will not exceed the upper limit. You can view the upper limit of the currently configured non-default static routes through show running-config

【Configuration Example]】 Set the maximum number of static routes to 900, and then restore the default value.

```
AC-FS(config)#ip static route-limit ?
  <1-10000> Value(default value: 1024) AC-
FS(config)# ip static route-limit 900 AC-
FS(config)# no ip static route-limit
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

2.6 maximum-paths

Configure the number of equal-cost routes.

maximum-paths number

Configure the default number of equal-cost routes.

no maximum-paths

Restore Default Configuration.

default maximum-paths

【Parameter Description】

Parameter	Description
number	The number of equal-cost routes, in the range 1-32.

【Default Configuration】 The default value is 32.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 The purpose of configuring the number of equal-cost routes is to control the number of equal-cost routes. After configuring the number of equal-cost routes through maximum-paths, the following effects will be produced. In load balancing mode, the number of branches for load balancing It will not exceed the configured number of equal-cost routes. You can view the number of currently configured equal-cost routes through show running config.

【Configuration Example]】Set up to 10 equal-cost routes, and then restore the default value.

```
AC-FS(config)# maximum-paths 10
AC-FS(config)# no maximum-paths
```

【Verification】 View the specific ecmp route through show ip route.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.7show ip route

View IP routing table information.

show ip route [[network [mask [longer-prefix]] | count | protocol [process-id] | weight]]

View IP routing table information according to routing ecmp attributes, etc.

show ip route [[normal | ecmp] [network [mask]]]

【Parameter Description】

Parameter	Description
network	(Optional) Only display routing information to the target network, all routes are displayed by default.
mask	(Optional) Only the route of the destination network with the mask is displayed, and the route with the longest matching prefix is displayed by default.
longer-prefix	(Optional) Display all detailed routes matching the specified prefix range
count	(Optional) Displays the current number of routes (for ECMP/WCMP routes, it is calculated by one route). By default, statistics on the number of routes are not displayed.

protocol	(Optional) Routing protocol or keywords: connected, static; when displaying a specific protocol route, use the following keywords: ospf, rip. All protocols are displayed by default.
process-id	(Optional) Process ID of the routing protocol. By default, all processes are displayed.
weight	(Optional) Only routes with non-default weights are displayed, and routes with all weights are displayed by default.
normal	(Optional) Displays common routes, does not display equal-cost routes, and displays all types of routes by default.
ecmp	(Optional) Only equal-cost routes are displayed, and all types of routes are displayed by default.

【Command Mode】 Privileged user mode, global configuration mode, interface configuration mode, routing protocol configuration mode, routing map configuration mode, etc.

【Default Level】 14

【Usage Guide】 This command can flexibly display the specified routing information according to the options.

show ip route is used to display the actual table entries that can be used for forwarding. If you want to see the table entries of various attributes, please specify normal | ecmp | fast-reroute Parameters.

【Configuration Example]】 1: The following is the display result of the show ip route command:

```
AC-FS# show ip route

Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area, * - candidate default
Gateway of last resort is no set
S........20.0.0.0/8 is directly connected, VLAN 1
S    22.0.0.0/8 [1/0] via 20.0.0.1
O E2 30.0.0.0/8 [110/20] via 192.1.1.1, 00:00:06, VLAN 1
R    40.0.0.0/8 [120/20] via 192.1.1.2, 00:00:23, VLAN 1
B  50.0.0.0/8 [120/0] via 192.1.1.3, 00:00:41
C    192.1.1.0/24 is directly connected, VLAN 1
C    192.1.1.254/32 is local host.
```

2: The following is the display result of the show ip route network command:

```
AC-FS# show ip route 30.0.0.0
Routing entry for 30.0.0.0/8
Distance 110,  metric  20
Routing Descriptor Blocks:
192.1.1.1, 00:01:11 ago, via VLAN 1, generated by OSPF, extern 2
```

3: The following is the display result of the show ip route count command:

```
AC-FS# show ip route count
————————— route info —————————
the num of active route: 5
```

4: The following is the display result of the show ip route weight command:

```
AC-FS# show ip route weight
-------------[distance/metric/weight] ---------------
S     23.0.0.0/8 [1/0/2] via 192.1.1.20
S  172.0.0.0/16 [1/0/4] via 192.0.0.1
```

5: The display result of the show ip route normal command:

```
        R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area, * - candidate default
Gateway of last resort is no set
S.......20.0.0.0/8 is directly connected, VLAN 1
S     22.0.0.0/8 [1/0] via 20.0.0.1
O E2  30.0.0.0/8 [110/20] via 192.1.1.1, 00:00:06, VLAN 1
R     40.0.0.0/8 [120/20] via 192.1.1.2, 00:00:23, VLAN 1
B   50.0.0.0/8 [120/0] via 192.1.1.3, 00:00:41
C     192.1.1.0/24 is directly connected, VLAN 1
C     192.1.1.254/32 is local host
```

6: The display result of the show ip route ecmp command:

```
AC-FS#show ip route ecmp

Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area, * - candidate default
Gateway of last resort is 192.168.1.2 to network 0.0.0.0
S*.....0.0.0.0/0 [1/0] via 192.168.1.2
               [1/0] via 192.168.2.2
O IA 192.168.10.0/24 [110/1] via 35.1.10.2, 00:38:26, VLAN 1
                           [110/1] via 35.1.30.2, 00:38:26, VLAN 3
```

7: The display result of the show ip route fast-reroute command:

```
AC-FS#show ip route fast-reroute

Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS, V - Overflow route
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area, * - candidate default
Status codes: m - main entry, b - backup entry, a - active entry

Gateway of last resort is 192.168.1.2 to network 0.0.0.0
```

```
S*.....0.0.0.0/0 [ma] via 192.168.1.2
               [b] via 192.168.2.2
O IA 192.168.10.0/24 [m] via 35.1.10.2, 00:38:26, VLAN 1
                     [ba]  via 35.1.30.2, 00:38:26, VLAN 3
```

8: The display result of the show ip route fast-reroute network command:

```
AC-FS# show ip route fast-reroute 30.0.0.0
Routing entry for 30.0.0.0/8
Distance 110, metric 20
Routing Descriptor Blocks:
[m] 192.1.1.1, 00:01:11 ago, via VLAN 1, generated by OSPF, extern 2
[ba]192.1.1.1, 00:01:11 ago, via VLAN 1, generated by OSPF, extern 2
```

Field Description:

Field	Description
O	Description The source routing protocol of this route. The possible values of this Field are: C: Directly connected route; L: local route; S: static route; R: RIP routing; B: BGP route; O: OSPF routing; I : IS-IS route.
E2	route type. The possible values of this Field are: E1: OSPF external route type 1; E2: OSPF external route type 2; N1: OSPF NSSA external route type 1; N2: OSPF NSSA external route type 2; SU: IS-IS summary route; L1: IS-IS level 1 routing; L2: IS-IS level 2 routing; IA: routing domain internal routing.
20.0.0.0/8	The network address and mask length of the destination network.
[1/0]	Administrative distance/metrics.
Via 20.0.0.1	next hop IP address.
00:00:06	Protocol route lifetime.
VLAN 1	Next-hop forwarding interface.
Routing Descriptor Blocks	Displays the next hop IP address of routing information, routing source, update time, via which interface, source routing protocol, type, BGP community attribute value, etc.

【Prompt Information】-

【Platform Description】 -

2.8show ip route summary

View statistics on a single routing table.

show ip route summary

View statistics for all routing tables.

show ip route summary all

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】 Use this command to view the statistics of the routing table.

【Configuration Example]】1: View the statistics of the global routing table.

```
AC-FS# show ip route summary
Codes:  NORMAL - Normal route  ECMP - ECMP route  FRR - Fast-Reroute route

    Memory: 2000 bytes
Entries: 22, based on route prefixes
                    NORMAL  ECMP    FRR     TOTAL
        Connected   3       0       0       3
        Static      2       1       1       4
        RIP         1       2       1       4
        OSPF            2           1           1           4
        ISIS            0           0           0           0
        BGP  0  0  0  0
        TOTAL       8       4       3       15
```

2: View the statistics of all routing tables.

```
 AC-FS# show ip route summary all
Codes:  NORMAL - Normal route  ECMP - ECMP route  FRR - Fast-Reroute route

IP          routing           table           count:1
Total
```

```
    Memory: 2000 bytes
    Entries: 22, based on route prefixes
                    NORMAL  ECMP    FRR     TOTAL
        Connected   3       0       0       3
        Static          2           1           1           4
        RIP             1           2           1           4
        OSPF            2           1           1           4
        ISIS  0  0  0  0
        BGP             0       0       0       0
        TOTAL       8       4       3       15
Global
    Memory: 2000 bytes
    Entries: 22, based on route prefixes
                    NORMAL  ECMP    FRR     TOTAL
        Connected   3       0       0       3
        Static      2       1       1       4
        RIP         1       2       1       4
        OSPF        2       1       1       4
        ISIS        0       0       0       0
        BGP         0       0       0       0
        TOTAL       8      4       3      15
```

Field Description:

Field	Description
NORMAL	The entry type of the Description category. The possible values of this Field are: NORMAL: Normal routing table entry (non-ECMP or FRR routing; ECMP: Equal-cost multi-path routing table entry; FRR: fast rerouting entry; TOTAL: The total of all types of table entries.
Memory	The size of the memory occupied by the current routing table.
Entries	The current routing table contains entry entries (based on entry prefix entries, not next hop entries).

Connected	DescriptionThe protocol type of the entry in this row. The possible values of this Field are: Connected: Directly connected routing entry Static: Static routing table entry RIP: RIP routing table entry OSPF: OSPF routing table entries ISIS: ISIS routing table entry BGP: BGP routing table entry TOTAL: total of all protocol entries
IP routing table count	number of routing tables.
Global	Description Current routing table name. The possible values of this Field are: Global: global TOTAL: total global routing table information

【Prompt Information】-

【Platform Description】 -

3 FPM

3.1 clear ip fpm counters

Clear FPM processing ipv4 packet loss count.

clear ip fpm counters

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】15

【Usage Guide】-

【Configuration Example]】1: Clear the FPM processing ipv4 packet loss count on the device

```
AC-FS# clear ip fpm counters
```

【Prompt Information】-

【Platform Description】 -

3.2ip session direct-trans-disable

The configuration does not allow transparent transmission of packets without creating a flow when the flow is full.

ip session direct-trans-disable

restore default settings.

no ip session direct-trans-disable

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 AC, AP products default when the flow table is full, it can implement the policy of not creating a flow for new connections and directly transparent transmission without accelerated processing.

【Command Mode】 Global configuration mode

【Default Level】15

【Usage Guide】-

【Configuration Example]】Setting the device is not allowed to transparently transmit packets without creating a flow when the device is full.

```
AC-FS(config)# ip session direct-trans-disable
```

【Verification】-

【Prompt Information】-

【Common Mistake】

【Platform Description】 -

3.3 ip session tcp-loose

Configure relaxed tcp state transition checking

ip session tcp-loose

restore default settings

no ip session tcp-loose

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 By default, loose tcp state transition check is performed.

【Command Mode】 Global configuration mode

【Default Level】15

【Usage Guide】-

【Configuration Example】Set the device to do loose tcp status check

```
AC-FS(config)# ip session tcp-loose
```

【Verification】-

【Prompt Information】-

【Common Mistake】

【Platform Description】 -

3.4 ip session tcp-state-inspection-enable

Configure not to do tcp state transition check.

ip session tcp-state-inspection-enable

restore default settings.

no ip session tcp-state-inspection-enable

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 AC and AP products do not perform tcp status tracking by default.

【Command Mode】 Global configuration mode

【Default Level】15

【Usage Guide】-

【Configuration Example]】Set the status tracking check of tcp enabled on the device

```
AC-FS(config)# ip session tcp-state-inspection-enable
```

【Verification】-

【Prompt Information】-

【Common Mistake】

【Platform Description】 -

3.5ip session threshold

Configure the number of packets allowed to be received by the flow

ip session threshold {icmp-closed | icmp-started | rawip-closed | tcp-syn-sent | tcp-syn-receive | tcp-closed | udp-closed} { num }

restore default settings

no ip session threshold {icmp-closed | icmp-started | rawip-closed | tcp-syn-sent | tcp-syn-receive | tcp-closed | udp-closed}

【Parameter Description】

Parameter	Description
icmp-closed	Set the number of packets passed by the flow whose protocol is ICMP status is closed, the default is 10 (1 - 2000000000).
icmp-started	Set the number of packets passed by the flow whose protocol is ICMP status is the start, the default is 300 (5 - 2000000000).
rawip-closed	Set the protocol to other ip protocol and the number of packets passing through the flow whose status is closed, the default is 10 (1 - 2000000000).
tcp-syn-sent	Set the number of packets passed by the flow whose protocol is TCP and the status is syn-send, 10 (5 - 2000000000).
tcp-syn-receive	Set the number of packets passed by the flow whose protocol is TCP and the status is syn-receive, the default is 20 (5 - 2000000000).
tcp-closed	Set the number of packets passed by the flow whose protocol is TCP and the status is closed, the default is 20 (5 - 2000000000).
udp-closed	Set the number of packets passed by the flow whose protocol is UDP and the status is closed, the

	default is 10 (1 - 2000000000).
num	Set the number of packets passed.

【Default Configuration】 The default value is used by default

【Command Mode】 Global configuration mode

【Default Level】15

【Usage Guide】 To make the current configuration take effect, you need to configure ip session track-state-strictly on the corresponding device.

【Configuration Example]】 Set the number of packets passed in the tcp closed state on the device to 100.

```
AC-FS(config)# ip session threshold tcp-closed 100
```

【Verification】

【Prompt Information】-

【Common Mistake】

【Platform Description】 -

3.6 ip session timeout

Configure aging time

ip session timeout {icmp-closed | icmp-connected | icmp-started | rawip-closed | rawip-connected | rawip-established | rawip-started | tcp-close-wait | tcp-closed | tcp-established | tcp-fin- wait1 | tcp-fin-wait2 | tcp-syn-receive | tcp-syn-sent | tcp-syn-sent2 | tcp-time-wait | udp-closed | udp-started | udp-connected | udp-established} { num }

restore default time

no ip session timeout {icmp-closed | icmp-connected | icmp-started | rawip-closed | rawip-connected | rawip-established | rawip-started | tcp-close-wait | tcp-closed | tcp-established | tcp-fin -wait1 | tcp-fin-wait2 | tcp-syn-receive | tcp-syn-sent | tcp-syn-sent2 | tcp-time-wait | udp-closed | udp-started | udp-connected | udp-established}

【Parameter Description】

Parameter	Description
icmp-closed	Set the death time of the stream whose protocol is ICMP status is closed, the default is 10s (5 – 60).
icmp-connected	Set the death time of the flow whose protocol is ICMP state is connected, the default is 10s (5 – 120).
icmp-started	Set the protocol as the death time of the stream whose status is ICMP, the default is 10s (5 - 120).
rawip-closed	Set the protocol to other ip protocol and the death time of the stream whose status is connected, the default is 10s (5 - 60).
rawip-connected	Set the protocol to other ip protocol and the death time of the stream whose status is connected, the default is 300s (10 - 300).
rawip-established	Set the protocol to other ip protocol and the death time of the established flow, the default is 300s (10 - 600).
rawip-started	Set the protocol to other ip protocol and the death time of the stream whose status is start, the default is 300s (10 - 300).
tcp-close-wait	Set the death time of the stream whose protocol is TCP and whose status is tcp-close-wait, the default is 30s (10 - 120).
tcp-closed	Set the death time of the stream whose protocol is TCP and the state is tcp-closed, default 10s (5 - 20).
tcp-established	Set the death time of a stream whose protocol is TCP and whose state is tcp-established, the default is 1800s (300 - 604800).
tcp-fin-wait1	Set the death time of the stream whose protocol is TCP and whose state is tcp-fin-wait1, the default is 60s (10 - 120).
tcp-fin-wait2	Set the death time of the stream whose protocol is TCP and whose state is tcp-fin-wait2, the default is 60s (10 - 120).
tcp-syn-receive	Set the death time of a stream whose protocol is TCP and whose state is tcp-syn-receive, default 10s (5 - 30).
tcp-syn-sent	Set the death time of a stream whose protocol is TCP and whose state is tcp-syn-sent, default 10s (5 - 30).
tcp-syn_sent2	Set the death time of a stream whose protocol is TCP and whose state is tcp-syn_sent2, default 10s (5-30).
tcp-time-wait	Set the death time of a stream whose protocol is TCP and whose state is tcp-time-wait, default 10s (5 - 60).
udp-closed	Set the death time of the stream whose protocol is UDP and the state is closed, the default is 10s (5 - 60).
udp-connected	Set the death time of the stream whose protocol is UDP and the state is connected, the default is 30s (10 - 300).
udp-established	Set the protocol to UDP and the death time of the established flow, the default is 600s (120 – 600).

udp-started	Set the death time of the stream whose protocol is UDP and whose status is start, default is 10s (10 - 300).
num	set death time.

【Default Configuration】 The default value is used by default.

【Command Mode】 Global configuration mode

【Default Level】15

【Usage Guide】-

【Configuration Example]】 Set the tcp established state stream death time on the device to 600s.

```
AC-FS(config)# ip session timeout tcp-established 600
```

【Verification】-

【Prompt Information】-

【Common Mistake】

【Platform Description】 -

3.7ip session track-state-strictly

Configure the flow status packet watermark check.

ip session track-state-strictly

restore default settings.

no ip session track-state-strictly

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 By default, the waterline check of flow status packets is not performed.

【Command Mode】 Global configuration mode

【Default Level】 15

【Usage Guide】 -

【Configuration Example]】Set the flow status packet waterline check on the device

AC-FS(config)# ip session track-state-strictly

【Verification】

【Prompt Information】-

【Common Mistake】

【Platform Description】 -

3.8 show ip fpm counters

View the packet loss count of ipv4 packets processed by FPM

show ip fpm counters

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】15

【Usage Guide】 Use this command to view the packet loss count information when FPM processes ipv4 packets. The upper part is the packet loss information for the packet, and the lower part is the flow information.

【Configuration Example]】 1: View the packet loss count of ipv4 packets processed by FPM.

```
AC-FS#sh ip fpm 1 2 counters
Dropped  packet  counters:
Count  Reason
0          Non-IPv4 packet
0          Bad IPv4 header length
0          Bad IPv4  total  length
0          Fragment pkt
0          change flow state notify FW refuse
0          Bad IPv4 checksum
0          Invalid IPv4 address
0          Invalid TCP flags
0          Invalid TCP sequence
0          Invalid ICMP message type
0          Invalid icmp initial message type
54         Invalid tcp init flags
0          Invalid tcp  connection  state
0          Connect over config threshold
0          Connect  has  been  terminated
0          Invalid egress fid
0          out of vfw session limit
0          Out of capability
<end>
Rejected or terminated connection counters:
Count  Reason
0          Out of life time
1968       Flow Terminated
0          Rejected by policy
```

<end>

Field Description:

Field	Description
count	Count.
Reason	Reason for packet loss.

【Prompt Information】-

【Platform Description】 -

3.9show ip fpm flows

View flow information of ipv4 packets.

show ip fpm flows

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】 15

【Usage Guide】 Use this command to view the flow information of ipv4 packets.

【Configuration Example]】 1: View the flow information of ipv4 packets.

```
AC-FS#show ip fpm flows
Pr  SrcAddr                          DstAddr                          SrcPort          DstPort
Vrf          SendBytes  RecvBytes  St    srcif                    dstif
ctrl_flag
```

Field Description:

Field	Description
Pr	Protocol.
SrcAddr	source address.
DstAddr	Destination address.
SrcPort	source port.
DstPort	destination port.
Vrf	vrf to which the source interface belongs.
SendBytes	Number of message bytes received in the request direction.
RecvBytes	Number of message bytes received in the reply direction.
St	current state of the stream.
srcif	source interface number.
dstif	destination interface number.
ctrl_flag	Flow Control Field.

【Prompt Information】 -

【Platform Description】 -

3.10 show ip fpm flows filter

Filter and view flow information of ipv4 packets.

show ip fpm flows filter protocol saddr smask daddr dmask

【Parameter Description】

Parameter	Description
protocol	ip protocol, the value range is 0 – 255.
saddr	Source ip address, the value range is all ip addresses.
smask	source ip address mask, value range 1 – 32.
daddr	Destination ip address, the value range is all ip addresses.
dmask	destination ip address mask, value range 1 – 32.

【Command Mode】 Privileged mode

【Default Level】15

【Usage Guide】 Use this command to filter and view the flow information of ipv4 packets.

【Configuration Example]】 1: View the flow information of ipv4 packets.

```
AC-FS#show ip fpm flows filter 1 192.168.1.1 32 192.168.2.1 30
Pr  SrcAddr                          DstAddr                          SrcPort          DstPort
Vrf          SendBytes  RecvBytes  St    srcif                  dstif
ctrl_flag
```

Field Description:

Field	Description
Pr	Protocol.
SrcAddr	source address.
DstAddr	Destination address.
SrcPort	source port.
DstPort	destination port.
Vrf	vrf to which the source interface belongs.

SendBytes	Number of message bytes received in the request direction.
RecvBytes	Number of message bytes received in the reply direction.
St	current state of the stream.
srcif	source interface number.
dstif	destination interface number.
ctrl_flag	Flow Control Field.

【Prompt Information】-

【Platform Description】 -

3.11 show ip fpm statistics

View ipv4 flow table statistics

show ip fpm statistics

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】15

【Usage Guide】 Use this command to view ipv4 flow table statistics

【Configuration Example]】1: View ipv4 flow statistics on eg device

```
AC-FS#show ip fpm statistics
The capacity of the flow table:150016.
Active flows num:109.
event count:65,
Fpm state inspection enable
```

Field Description:

Field	Description
The capacity of the flow table	Total flow meters.

Active flows num	Number of active flow tables.
event count:65,	Current event count.
Fpm state inspection enable	Status tracking table.

【Prompt Information】-

【Platform Description】 -

4 ROUTE-DB

4.1route-auto-choose

Configure an address library command.

route-auto-choose { cnc | cnii | cernet | cmcc | word } interface next-hop [tag num] [distance]

Delete an address library configuration.

no route-auto-choose { cnc | cnii | cernet | cmcc | word } interface next-hop [tag num] [distance]

Restore Default Configuration.

default route-auto-choose { cnc | cnii | cernet | cmcc | word } interface next-hop [tag num] [distance]

【Parameter Description】

Parameter	Description
cnc	Configure the China Unicom address library.
cnii	Configure Telecom Address Library
cernet	Configure the education network address database.
cmcc	Configure the mobile address library.
word	Configure other types of address libraries
interface	The outbound interface of the route corresponding to the address library.
next-hop	The next hop ip of the route corresponding to the address library.
tag num	The tag of the route corresponding to the address library.
distance	The metric value of the address library route.

【Default Configuration】 This function is disabled by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 By configuring this command, you can specify the address library associated with a specific interface.

【Configuration Example】1: Configure an address library command to enable telecom address library, the interface is gigabitEthernet 0/1, and the next hop address is 202.100.12.5.

```
AC-FS# config
AC-FS(config)# route-auto-choose cnii gigabitEthernet 0/1 202.100.12.5
```

【Verification】 Use the show route-db-info cnii command to view the corresponding telecom address database information.

【Prompt Information】 1: If the next hop of the address library is configured as the device ip, the corresponding information will be prompted.

```
AC-FS(config)#route-auto-choose cmcc gi 0/5 192.168.55.111
%Invalid next hop address (it's this router)
```

【Common Mistake】-

【Platform Description】 -

4.2route-auto-choose update

Update the address library file. After executing the command, update the address library being executed according to the current address library file, so that the file can be configured and used immediately after the file is updated.

route-auto-choose update

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to update the address library.

【Configuration Example]】1: Update the address library file.

```
AC-FS# config
AC-FS(config)# route-auto-choose update
```

【Prompt Information】-

【Platform Description】 -

4.3 route-auto-choose user-defined

Add custom address library command:

route-auto-choose user-defined name string [ip_address ip_mask]

Command to delete custom address library.

no route-auto-choose user-defined name string [ip_address ip_mask]

Upgrade the custom library information through the custom library file in the specified format on the device.

route-auto-choose user-defined update file_path

【Parameter Description】

Parameter	Description
string	The name of the custom address library.
ip_address	The IP of the custom address library.
ip_mask	Mask of custom address library.
file_path	The absolute path of the custom address library upgrade file in the shell directory.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command can be used to add a custom address library or upgrade the custom address library.

【Configuration Example]】1: Create and add a custom address library named test1 with ip 1.2.3.0 and mask 255.255.255.0

```
AC-FS# config
AC-FS(config)# route-auto-choose user-defined name test1 1.2.3.0 255.255.255.0
```

【Verification】Use the show route-db-info user-defined command to view the information of the added custom address library.

【Prompt Information】 1: If the information of a custom address library is configured repeatedly, the following information will be prompted.

```
AC-FS(config)#route-auto-choose user-defined name test1
No need to create "test1": already exists
AC-FS(config)#route-auto-choose user-defined name test1 1.2.3.0 255.255.255.0
1.2.3.0 255.255.255.0 already exists in "test1"
```

2: The ip of the private network and some other special network segments cannot be added to the custom address library. If it is added, the following information will be displayed

```
AC-FS(config)#route-auto-choose user-defined name test1 10.2.3.0 255.255.255.0
Invalid ip or mask detected! Please check again.
```

【Platform Description】 -

4.4 show route-db-info

View address library information command.

show route-db-info { cnc | cnii | cernet | cmcc | word | db-type | ip_address | user-defined }

【Parameter Description】

Parameter	Description
cnc	Query Unicom Address Database Information.
cnii	Query Telecom Address Database Information.
cernet	Query Education Network Address Database Information.
cmcc	Query mobile address database information.
word	Query other types of address library information.
db-type	Query how many carrier types are in the current address library file.
ip_address	Query the carrier type to which an ip belongs.
user-defined	Query user-defined address library information.

【Command Mode】 All modes

【Default Level】 14

【Usage Guide】 You can query the address library information.

【Configuration Example】Query all carrier types in the address database

```
AC-FS# show route-db-info db-type
```

【Verification】 Displays the number of operator types in the current address database file, there are three columns in total, the first column is the letter abbreviation, the second column is the Chinese abbreviation, and the third column is the address database version of each operator.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

Chapter 9 Security

This volume introduces the relevant content of the Security Command Manual, including the following chapters:

1. Web authentication configuration command
2. AAA
3. RADIUS
4. 802.1x
5. ARP Check
6. Anti-gateway APR spoofing
7. Global IP+MAC binding
8. DHCP Snooping
9. IP Source Guard
10. DNS SNOOPING
11. IGMP Snooping
12. ACL
13. SCC
14. PASSWORD-POLICY
15. SSH
16. CONTENT-AUDIT
17. IPSEC-IKE
18. VPDN
19. Advertisement Configuration Commands

1 Web Authentication Configuration Commands

1.1accounting

Sets the accounting method for the template.

accounting { method-list }

Reset to default accounting method.

no accounting

【Parameter Description】

Parameter	Description
method-list	Method list name.

【Default Configuration】 The default method is used by default.

【Command Mode】 Template configuration mode.

【Default Level】 14

【Usage Guide】 The method list name in this command needs to be consistent with the network accounting method list name configured in AAA.

【Configuration Example]】1: Specify the eportalv2 template to use the mlist1 accounting method.

```
AC-FS(config.tmplt.eportalv2)# accounting mlist1
```

【Verification】Use show web-auth template to view the currently configured template Parameter

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.2authentication

Set the authentication method for the template.

authentication { method-list }

Reset to default authentication method.

no authentication

【Parameter Description】

Parameter	Description
method-list	Method list name.

【Default Configuration】 The default method is used by default.

【Command Mode】 Template configuration mode.

【Default Level】 14

【Usage Guide】 The method list name in this command needs to be consistent with the web authentication method list name configured in AAA.

First-generation authentication does not support method list configuration。

【Configuration Example]】1: Specify the eportalv2 template to use the mlist1 authentication method.

```
AC-FS(config.tmplt.eportalv2)#authentication mlist1
```

【Verification】Use show web-auth template to view the currently configured template Parameter

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.3bindmode

Set the template binding mode.

bindmode {ip-only-mode }

Reset template binding mode.

no bindmode

【Parameter Description】

Parameter	Description
ip-only-mode	In IP only mode, only the IP information is sent to the forwarding table; in the three-layer network, the MAC information is not accurate, it is recommended to use this mode.

【Default Configuration】-

【Command Mode】 Template configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Specify the binding mode of the eportalv2 template as IP-only mode.

```
AC-FS(config.tmplt.eportalv2)# bindmode ip-only-mode
```

【Verification】Use show web-auth template to view the currently configured template Parameter

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.4 clear web-auth acl

Remove all web black and white list configurations on the device.

clear web-auth acl [white-url | black-url | black-ip | black-port]

【Parameter Description】

Parameter	Description
white-url	Specifies to remove only all whitelisted URLs.

black-url	Specifies to delete only all blacklisted URLs.
black-ip	Specifies to delete only all blacklisted Ips.
black-port	Specifies to delete only all blacklisted ports.

【Command Mode】 Privileged mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】 1: Delete all black and white list configurations

```
AC-FS# clear web-auth acl
```

【Prompt Information】-

【Platform Description】 -

1.5 clear web-auth direct-arp

Delete all arp resources on the device.

clear web-auth direct-arp

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】 1: Delete all direct arp resources.

```
AC-FS# clear web-auth direct-arp
```

【Prompt Information】-

【Platform Description】 -

1.6 clear web-auth direct-host

Delete all authentication-free users on the device.

clear web-auth direct-host

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Delete all authentication-free users.

```
AC-FS# clear web-auth direct-host
```

【Prompt Information】-

【Platform Description】 -

1.7 clear web-auth direct-site

Delete all authentication-free network resources on the device.

clear web-auth direct-site

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Delete all authentication-free network resources

```
AC-FS# clear web-auth direct-site
```

【Prompt Information】-

【Platform Description】 -

1.8 clear web-auth group

Delete all group information on the device.

clear web-auth group

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Delete all group information

```
AC-FS# clear web-auth group
```

【Prompt Information】-

【Platform Description】 -

1.9 clear web-auth user

Force the user to go offline on the device.

clear web-auth user { all | ip ip-address | mac mac-address | name name-string | session-id num }

【Parameter Description】

Parameter	Description
ip-address	Specifies the user's IPv4 address.
mac-address	Specifies the user's MAC address.
name-string	specify username.
num	AAA session ID for the specified user.

【Command Mode】 Privileged mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】 1: Force all users to log off.

```
AC-FS# clear web-auth user all
```

【Prompt Information】-

【Platform Description】 -

1.10escape interval

Set the single escape function of WeChat connected to wifi authentication.

escape interval seconds online-time minutes

Disable the single escape function of WeChat connected to wifi authentication.

no escape interval

【Parameter Description】

Parameter	Description
seconds	Configure an escape decision timer to allow users to escape after the timer expires without receiving a login authorization request. Unit: seconds, recommended value is 5s.

minutes	Configure the amount of time available to escape users. Unit: minutes, 0 means no limit to the available time

【Default Configuration】 There is no configuration by default.

【Command Mode】 Template configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Configure escape function

```
AC-FS(config.tmplt.wechat)# escape interval 5 online-time 10
```

【Verification】 Use show web-auth template to view the currently configured template parameter.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.11escape user-try-auth

Set the single escape function of WeChat connected to wifi authentication version 3.0.

escape user-try-auth counts online-time minutes

Disable the single escape function of WeChat connected to wifi authentication.

no escape user-try-auth

【Parameter Description】

Parameter	Description
counts	Configure the number of times the user tries to click WeChat authentication, and let the user escape if the configured number of times is still not online. Unit: times, the recommended value is 4 times.

minutes	Configure the available time for escape users. Unit: minutes.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Template configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Configure escape function

```
AC-FS(config.tmplt.wechat)#escape user-try-auth 4 online-time 15
```

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.12domain

The second generation automatically adds domain information to the username

domain domain-string

【Parameter Description】

Parameter	Description
domain-string	Specifies an automatically added domain information string.

【Command Mode】 Web authentication template configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】 1: Configure automatic addition of domain information.

```
AC-FS(config.tmplt.eportalv2)#domain @wifi
```

【Prompt Information】-

【Platform Description】 -

1.13fmt

In the 2nd generation template configuration mode, set the url format of the redirection message.

fmt { cmcc-ext1 | cmcc-ext2 | cmcc-mtx | cmcc-normal | cmcc-ext3 | ct-jc | cucc | AC-FS | custom }

In the 1st generation template configuration mode, set the url format of the redirection packet.

fmt { ace | AC-FS | custom }

Customized URL format, set the URL format under the 1st generation and 2nd generation templates.

fmt custom [encry { md5 | des | des_ecb | des_ecb3 | none }] [user-ip userip-str] [user-mac usermac-str mac-format [dot | line | none]] [user-vid uservid-str] [user-id userid-str] [nas-ip nasip-str] [nas-id nasid-str] [nas-id2 nasid2-str] [ac-name acname-str] [ap-mac apmac-str mac-format [dot | line | none]] [url url-str] [ssid ssid-str] [port port-str] [ac-serialno ac-sno-str] [ap-serialno ap-sno-str] [additional extern-str]

Delete configuration.

no fmt custom [user-ip][user-mac][user-vid][user-id][nas-ip][nas-id][nas-id2][ac-name][ap-mac][url] [ssid] [port] [ac-serialno] [ap-serialno] [additional]

【Parameter Description】

Parameter	Description
ace	Support ACE linkage.
AC-FS	FS url format.
custom	Customized format.
userip-str	Parameter name corresponding to user ip.
usermac-str	The Parameter name corresponding to the user's mac.
uservid-str	Parameter name corresponding to user vid.
userid-str	The Parameter name corresponding to the user id.
nasip-str	The Parameter name corresponding to the device ip.
nasid-str	Parameter name corresponding to the NAS device ID.
nasid2-str	Parameter name corresponding to the NAS device ID (two nasid parameters can be customized).

ac-name	The Parameter name corresponding to the device name.
apmac-str	Parameter name corresponding to the MAC address of the associated AP.
url-str	The Parameter name corresponding to the user's original access url.
ssid-str	Parameter name corresponding to the SSID.
port-str	Parameter name corresponding to the user authentication port.
ac-sno-str	Parameter name corresponding to the serial number of the ac device.
ap-sno-str	Parameter name corresponding to the serial number of the ap device.
extern-str	Fixed strings, some portals require some specific string identifiers.
md5	The configured Parameter is encrypted with md5.
des	The configured Parameter adopts des encryption.
des_ecb	The configured Parameter is encrypted by des_ecb.
des_ecb3	The configured Parameter is encrypted with des_ecb3.
none	The configured Parameter is not encrypted and is transmitted in plain text.

【Default Configuration】 The default is AC-FS format.

【Command Mode】 Template configuration mode.

【Default Level】 14

【Usage Guide】 According to the connection specification of the portal server, set different url types.

The 10.x operator version is to use the global command http redirect url-fmt {cmcc-normal | cmcc-ext1 | cmcc-ext2} to set the url Types of. 11.x obsolete this command and make it hidden. If the user executes this command, it will be saved as the fmt configuration command under the template.

【Configuration Example]】 1: Set the redirect url as the extension type of China Mobile.

```
AC-FS(config.tmplt.eportalv2)#fmt cmcc-ext1
```

【Verification】 Use show web-auth template to view the configured template.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.14 free-auth

Set the authentication-free function of WeChat connected to wifi authentication.

free-auth pc

Delete the ip of the device authenticated by WeChat connected to wifi.

no free-auth

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 There is no configuration by default.

【Command Mode】 Template configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Configure pc terminal without authentication.

```
AC-FS(config.tmplt.wechat)#free-auth pc
```

【Verification】 Use show web-auth template to view the currently configured template parameter.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.15gateway-id

Set the value of gw_id in the wifidog standard protocol in the interaction between the wifidog authenticated device and the server.

gateway-id string

Delete the value of gw_id in the wifidog standard protocol in the interaction between wifidog authenticated devices and servers.

no gateway-id

【Parameter Description】

Parameter	Description
string	Configure the device and server to use the value of gw_id in the wifidog protocol field.

【Default Configuration】 Default Configuration is the serial number of the device.

【Command Mode】 Template configuration mode

【Default Level】 14

【Usage Guide】 Default Configuration is the serial number of the device. If there is no special docking requirement, you do not need to configure it manually. However, in the hot standby and VAC scenarios, multiple devices are externally reflected as one device, so they must be configured.

【Configuration Example]】1: Configure the device and server to use the wifidog protocol. The value of gw_id in the Field is 14144b6fb807

```
AC-FS(config.tmplt.wifidog)#gateway-id 14144b6fb807
```

【Verification】Use show running-config to view the currently configured template Parameter

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.16 http redirect adapter ios

Configure WeChat authentication IOS automatic popup control commands.

http redirect adapter ios

Delete configuration.

no http redirect adapter

【Parameter Description】-

【Default Configuration】 No configuration.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure WeChat authentication IOS automatic popup control commands.

```
AC-FS(config)# http redirect adapter ios
```

【Verification】Use show running-config to view the current configuration

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.17 http redirect direct-arp

Set the passthrough ARP address range.

http redirect direct-arp { ip-address [ip-mask] }

Delete configuration.

no http redirect direct-arp { ip-address [ip-mask] }

【Parameter Description】

Parameter	Description
ip-address	IPv4 address.
ip-mask	(Optional) IPv4 address mask.

【Default Configuration】 By default, no pass-through ARP resource is set.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】When the ARP CHECK function is enabled, the ARP learning function is controlled, and the user cannot learn the ARP of the gateway and other devices. In this case, you need to use this command to release the ARP learning of the specified address/network segment.

【Configuration Example]】1: Set the website whose IP address is 172.16.0.1 as a pass-through ARP resource.

```
AC-FS(config)# http redirect direct-arp 172.16.0.1
```

【Verification】Use show web-auth direct-arp to view the configured pass-through ARP address range

【Prompt Information】 1: Illegal IP/mask format.

```
%Error: Invalid IP address.
```

【Common Mistake】-

【Platform Description】 -

1.18 http redirect direct-site

Set the authentication-free network resource scope.

http redirect direct-site { ipv6-address | ipv4-address [ip-mask] [arp] }

Delete the authentication-free network resource scope.

no http redirect direct-site { ipv6-address | ipv4-address [ip-mask] }

【Parameter Description】

Parameter	Description
Ipv6-address	The IPv6 address of the authentication-free network resource.
Ipv4-address	The IPv4 address of the authentication-free network resource.
ip-mask	(Optional) The IPv4 address mask of the authentication-free network resource.
arp	(Optional) If the ARP CHECK function is enabled on the device, ARP binding needs to be performed on the authentication-free network resource range, and the arp keyword needs to be configured. Required only when setting up IPv4 network resources.

【Default Configuration】 By default, no authentication-free network resources are set.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】 After enabling Web authentication, all users need to pass Web authentication before they can access network resources. To open some network resources, unauthenticated users can also access these open network resources, use this command. When a website is an authentication-free network resource, all users can access the website.

A maximum of 50 authentication-free network resource ranges are allowed to be configured

【Configuration Example]】 1: Set the website whose IP address is 172.16.0.1 as a network resource for authentication-free access.

```
AC-FS(config)# http redirect direct-site 172.16.0.1
```

【Verification】 Use show web-auth direct-site to view the range of configured authentication-free network resources

【Prompt Information】 1: Illegal IP/mask format.

```
%Error: Invalid IP address.
```

【Common Mistake】 -

【Platform Description】 -

1.19 http redirect port

Set to redirect the HTTP WEB request of the specific destination port number sent by the user.

http redirect port port-num

Remove redirection of HTTP WEB requests to a specific destination port number.

no http redirect port port-num

【Parameter Description】

Parameter	Description
port-num	The destination port number of HTTP WEB requests.

【Default Configuration】 By default, HTTP packets of port 80 sent by users are intercepted.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】 1. When a user accesses network resources, the user will send HTTP packets, and the device intercepts the HTTP packets from the user to determine whether the user is accessing network resources; when the device detects that an unauthenticated user is When accessing network resources, users will be blocked from accessing network resources, and an authentication page will pop up for users.

2. By default, the device detects whether users are accessing network resources by intercepting HTTP packets with port number 80 sent by users.

3. To change the device to intercept HTTP packets of a specific port number sent by the user, use this command.

4. A maximum of 10 different destination port numbers are allowed, and the port number 80 is also included in the total number range.

【Configuration Example]】1: Redirect the HTTP WEB request with port number 8080 sent by the user.

```
AC-FS(config)# http redirect port 8080
```

2: Do not redirect HTTP WEB requests with port number 80 sent by users.

```
AC-FS(config)# no http redirect port 80
```

【Verification】 Use show web-auth rdport to view the current port listening status

【Prompt Information】 1: Blocking well-known protocol ports, such as 23, is not allowed.

```
%Error: Can't set local reserved port(23) as redirection port.
```

【Common Mistake】-

【Platform Description】 -

1.20http redirect session-limit

Sets the global maximum number of HTTP sessions for the same unauthenticated user, or the total number of HTTP sessions for unauthenticated users per port.

http redirect session-limit session-num [port port-session-num]

Recover the maximum number of HTTP sessions for unauthenticated users.

no http redirect session-limit

【Parameter Description】

Parameter	Description
session-num	The global maximum number of HTTP sessions for the same unauthenticated user, ranging from 1 to 255.
port-session-num	(Optional) The total number of HTTP sessions of unauthenticated users under each port, in the range of 1-65535.

【Default Configuration】The default global maximum number of HTTP sessions per unauthenticated user is 255, and the maximum total number of HTTP sessions for unauthenticated users under each port is 300.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】 To prevent unauthenticated users from launching HTTP attacks and exhausting the device's TCP connections, you need to limit the maximum number of HTTP sessions for unauthenticated users on the device.
Since the user will occupy an HTTP session during authentication, and other applications of the user may also occupy the HTTP session, it is not recommended to set the maximum number of HTTP sessions for unauthenticated users to 1.

【Configuration Example]】 1: Set the maximum number of HTTP sessions for unauthenticated users to 4.

```
AC-FS(config)# http redirect session-limit 4
```

【Verification】Use the show web-auth parameter command to view the configuration parameter

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.21http redirect timeout

Sets the timeout period for maintaining redirected connections.

http redirect timeout seconds

Resume maintains a timeout of 3 seconds for redirected connections.

no http redirect timeout

【Parameter Description】

Parameter	Description
seconds	Sets the timeout period for maintaining the redirected connection; seconds, the value range is 1-10.

【Default Configuration】 The default timeout for maintaining the redirection connection is 3 seconds.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Set the timeout period for maintaining the redirection connection. Because after the three-way handshake is successful, you need to wait for the HTTP GET/HEAD message sent by the user, and then reply to the HTTP redirect message before closing the connection. Setting this limit can prevent users from not sending GET/HEAD packets and occupying the TCP connection for a long time.

【Configuration Example]】1: Set the timeout period for maintaining the redirection connection to 4.

```
AC-FS(config)# http redirect timeout 4
```

【Verification】Use the show web-auth parameter command to view the configuration parameter

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.22 http-method post

Specify the http method of the authentication request for clearpass authentication, as well as the username, password, and parameter name of the url before authentication.

http-method post [init-url-key init-string | username-key username-string | password-key password-string | password-encrypt { none | uam }]

Restore the http method of the authentication request to the default Parameter name.

no http-method post

【Parameter Description】

Parameter	Description
Init-string	Configure the Parameter name of the url address passed by clearpass before user authentication.
username-string	Configure the Parameter name of the username Parameter passed by clearpass.
password-string	Configure the Parameter name of the login password Parameter passed by clearpass.
uam	Encrypt password with ascii code.
none	Use clear text passwords.

【Default Configuration】 By default, the post method is used, the username parameter name is username, the password parameter name is password, and the url parameter name accessed before authentication is url. Password encryption method is none, no encryption.

【Command Mode】 Template configuration mode

【Default Level】 14

【Usage Guide】 In the default configuration, the user information Parameter in the authentication request packet is username=xxx&password=xxx.

【Configuration Example]】1: Set the username Parameter name to name, and the password Parameter name to pass.

```
AC-FS(config.tmplt.cpweb)# http-method post username-key name password-key pass
```

【Verification】Use the show running-config command to view the configuration Parameter

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.23ip

To configure the IP address function of the portal server, execute the command ip in template configuration mode.

ip { ip-address }

Clear the IP address for HTTP redirection.

no ip

【Parameter Description】

Parameter	Description
ip-address	The IPv4 address of the portal server.

【Default Configuration】 By default, the IP address of the portal server is not set.

【Command Mode】 Template configuration mode

【Default Level】 14

【Usage Guide】 This command replaces the original http redirect [ip-address] command; the original command is hidden and implemented as a compatible command.

【Configuration Example]】 1: Specify the IP address of the eportalv1 template as 172.16.0.1.

```
AC-FS(config.tmplt.eportalv1)#ip 172.16.0.1
AC-FS(config.tmplt.eportalv1)#
```

【Verification】Use show web-auth template to view the currently configured template parameter.

【Prompt Information】 1: It is not allowed to directly modify the server IP address.

```
%Error: Modify portal ip is unsupportted.
```

2: Setting illegal IP is not allowed.

```
%Error: Invalid portal ip address.
```

【Common Mistake】-

【Platform Description】 -

1.24ip portal source-interface

Specifies the portal communication port.

ip portal source-interface interface-type interface-num

Restore default configuration.

no ip portal source-interface

【Parameter Description】

Parameter	Description
interface-type	Interface type.
interface-num	interface index.

【Default Configuration】 No configuration.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Use the aggregation port as the portal communication port.

```
AC-FS (config)# ip portal source-interface Aggregateport 1
```

【Verification】Use show running-config to view the current configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.25iportal nat enable

Configure the built-in web authentication to support the NAT function.

iportal nat enable

Restore default configuration.

no iportal nat enable

【Parameter Description】-

【Default Configuration】 No configuration.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Enable built-in web authentication to support NAT function.

AC-FS (config)# iportal nat enable

【Verification】Use show running-config to view the current configuration

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.26iportal retransmit

Configure the built-in web authentication http connection retransmission times.

iportal retransmit times

Restore default configuration.

no iportal retransmit

【Parameter Description】

Parameter	Description
times	number of retransmissions

【Default Configuration】 The default is 3 times.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】 1: Configure the number of http connection retransmissions to 5 times.

```
AC-FS (config)# iportal retransmit 5
```

【Verification】Use show running-config to view the current configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.27iportal service

Configure the service template used by the built-in web authentication.

iportal service [internet internet-name] [local local-name]

Restore default configuration.

no iportal service [internet internet-name] [local local-name]

【Parameter Description】

Parameter	Description
internet-name	external service name.
local-name	local service name.

【Default Configuration】 No configuration.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the built-in web authentication local service name.

```
AC-FS (config)# iportal service local local-srv
```

【Verification】Use show running-config to view the current configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.28iportal user-agent

Configure the terminal name corresponding to the user UA Field.

iportal user-agent ua-name type mobile ua-string

Delete configuration.

no iportal user-agent ua-name type mobile ua-string

【Parameter Description】

Parameter	Description
ua-name	UA Field Name
ua-string	UA Field corresponding string

【Default Configuration】 No configuration.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】 The command is invalid, and the terminal identification function is used to realize it.

【Configuration Example】-

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.29key

Set the encryption key for the communication between the device and the server that is authenticated by WeChat connected to wifi.

key key-string

Delete the encryption key for the communication between the device and the server authenticated by WeChat connected to wifi.

no key

【Parameter Description】

Parameter	Description
key-string	Encryption key for communication between wifi-authenticated devices and servers.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Template configuration mode.

【Default Level】 14

【Usage Guide】

【Configuration Example]】1: Configure the encryption key for communication between the device and the server to be AC-FS

```
AC-FS(config.tmplt.wechat)#key AC-FS
```

【Verification】Use show web-auth template to view the currently configured template Parameter

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.30 login-popup

Set the pre-authentication advertising address.

login-popup url-string

Delete the pre-certification advertising address.

no login-popup

【Parameter Description】

Parameter	Description
url-string	Advertising address link.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Template configuration mode.

【Default Level】 14

【Usage Guide】

【Configuration Example]】1: Configure the pre-authentication advertisement page

```
AC-FS(config.tmplt.iportal)#login-popup http://www.AC-FS.com.cn
```

【Verification】Use show web-auth template to view the currently configured template Parameter

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.31 login-success response

Set the jump address after clearpass authentication is successful.

login-success response { msg success-msg | redirect-init-url [default-url def-url] | redirect-url url-string }

Delete the redirected address after successful authentication.

no login-success response

【Parameter Description】

Parameter	Description
successl-msg	The message prompted after the authentication is successful.
url-string	The url address to jump after the authentication is successful.
def-url	The default url to jump to after successful authentication. When clearpass does not carry the url accessed before authentication, the configured url address will be used.

【Default Configuration】 The default return success-msg.

【Command Mode】 Template configuration mode

【Default Level】 14

【Usage Guide】 When configuring default-url, if clearpass does not carry the address accessed before user authentication, use the address of this default-url.

【Configuration Example]】1: Jump to http://www.AC-FS.com.cn after successful configuration authentication.

```
AC-FS(config.tmplt.cpweb)#login-success redirect-url http://www.AC-FS.com.cn
```

【Verification】Use show web-auth template to view the currently configured template parameter.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.32 logout-popup-window

Set the clearpass authentication successfully and display the offline page.

logout-popup-window

After the authentication is successful, the logout page will not be displayed.

no logout-popup-window

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 By default, the offline page is not displayed.

【Command Mode】 Template configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Jump to the offline page after successful configuration authentication

```
AC-FS(config.tmplt.cpweb)#logout-popup-window
```

【Verification】 Use show web-auth template to view the currently configured template parameter.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.33nas-ip

Set the access service ip of wifidog or WeChat connected to wifi authentication, which is used for the server to initiate communication to this ip.

nas-ip { ip-address }

Delete the access service ip of wifidog or WeChat connected to wifi authentication.

no nas-ip

【Parameter Description】

Parameter	Description
ip-address	The access service ip of Wifidog or WeChat connected to wifi authentication is used for the server to initiate communication to this ip.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Template configuration mode

【Default Level】 14

【Usage Guide】 The configured access service ip cannot be set as a pass-through address

When the access service ip is configured as the device ip, the terminal under this authentication template will be intercepted by the device and forwarded to the server when accessing this ip, so that the device's web management interface cannot be accessed.

If the terminal under this authentication template needs to directly access this ip to manage this device, you can set this access service ip to an unused virtual service ip, such as 1.1.1.1, 2.2.2.2, etc.

【Configuration Example】1: Configure access service ip

```
AC-FS(config.tmplt.wifidog)#nas-ip 1.2.3.4
```

【Verification】 Use show web-auth template to view the currently configured template Parameter

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.34nas-port-id

Set the NAS-PORT-ID Parameter of a single AP.

nas-port-id string

Delete the NAS-PORT-ID Parameter of a single AP.

no nas-port-id

【Parameter Description】

Parameter	Description
string	Parameter name of nas-port-id

【Default Configuration】 There is no configuration by default.

【Command Mode】 AP configuration mode.

【Default Level】 14

【Usage Guide】 NAS-PORT-ID can only be configured on a single AP basis.

【Configuration Example]】 1: NAS-PORT-ID configuration

```
AC-FS(config)# ap-config ap740
AC-FS(config-ap)# nas-port-id guangdongyidong
```

【Verification】 Use show ap-config running to view the currently configured NAS-PORT-ID.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.35online-popup

Set the user's online popup advertisement address.

online-popup url-string

Delete the user's online popup advertisement address.

no online-popup

【Parameter Description】

Parameter	Description
url-string	Advertising address link.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Template configuration mode.

【Default Level】 14

【Usage Guide】

【Configuration Example]】1: Configure the post-authentication advertisement page

AC-FS(config.tmplt.iportal)#online-popup http://www.AC-FS.com.cn

【Verification】Use show web-auth template to view the currently configured template Parameter

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.36 page-suite

Set the built-in authentication page package.

page-suite filename

Deletes the specified page package.

no page-suite

【Parameter Description】

Parameter	Description
Filename	The filename of the page package.

【Default Configuration】 By default, the page package that comes with the device is used.

【Command Mode】 Template configuration mode.

【Default Level】 14

【Usage Guide】 The page package needs to be downloaded to the portal/zip directory of FLASH in advance.

【Configuration Example]】1: Specify the built-in page package

```
AC-FS(config.tmplt.iportal)#page-suite AC-FSpage
```

【Verification】Use show web-auth template to view the currently configured template Parameter

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.37port

Set the interactive port of the portal server.

port { port-num }

Reset the server port to the default port number.

no port

【Parameter Description】

Parameter	Description
port	Portal server communication port number. If it is built-in authentication, this port is the http port that the local machine listens on.

【Default Configuration】 The default port number is 50100, which is based on the UDP protocol.

【Command Mode】 Template configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Specify the port number of the eportalv2 server as 10000.

```
AC-FS(config.tmplt.eportalv2)#port 10000
```

【Verification】Use show web-auth template to view the currently configured template Parameter

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.38 redirect

Set the redirection packet format.

redirect { http | js }

Restore the default redirection method.

no redirect

【Parameter Description】

Parameter	Description
http	Use HTTP 302 protocol for url redirection.
js	Use HTTP 200 message, with js script for url jump.

【Default Configuration】 The default Ruijie format adopts js, and the cmcc related format adopts js.

【Command Mode】 Template configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Specify the redirect packet format as http.

```
AC-FS(config.tmplt.eportalv2)#redirect http
```

【Verification】Use show web-auth template to view the currently configured template Parameter

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.39 service-url

Set the server address of WeChat connected to wifi authentication.

service-url url-string

Delete the server address of WeChat connected to wifi authentication.

no service-url

【Parameter Description】

Parameter	Description
url-string	The server address of WeChat connected to wifi authentication.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Template configuration mode

【Default Level】 14

【Usage Guide】 The configured server address can be in the form of ip or domain name, and cannot start with http:// or https://.

【Configuration Example】1: The address of the configuration server is wmc.AC-FS.com.cn

```
AC-FS(config.tmplt.wechat)#service-url wmc.AC-FS.com.cn
```

【Verification】Use show web-auth template to view the currently configured template parameter.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.40 show web-auth acl

Displays the black and white list configuration.

show web-auth acl [balck-ip | black-port | black-url | white-url]

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Used to check the black and white list configuration of web authentication.

【Configuration Example】1: Display the black and white list configuration.

```
AC-FS# show web-auth acl
Black URL List:0
_________________________________________________________

Black IP List:0
_________________________________________________________

White URL List:0
_________________________________________________________
```

Field Description:

Field	Description
Black URL List	Blacklist URLs.
Black IP List	Blacklist IP.
White URL List	Whitelist URLs.

【Prompt Information】-

【Platform Description】 -

1.41 show http redirect

Displays pass-through and authentication-free configuration information.

show http redirect

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】Used to view the configuration of pass-through and authentication-free web authentication.

【Configuration Example】1: Display the pass-through and authentication-free configuration.

```
AC-FS# show http redirect
HTTP redirection settings:
  server..... 192.168.197.79
  port:          80 443
  homepage:      http://192.168.197.79:8080/eportal/index.jsp
  session-limit: 255
  timeout:  3
Direct sites: 3
  Address         Mask            ARP Binding
  --------------- --------------- -----------

  192.168.5.120   255.255.255.255 Off
  192.168.58.112  255.255.255.255 Off
  192.168.197.0     255.255.255.0     Off
Direct arps: 0
  Address         Mask
  --------------- ---------------

Direct hosts: 0
  Address         Mask            Port            ARP Binding
  --------------- --------------- --------------- -----------
```

Field Description:

Field	Description
HTTP redirection settings	Redirect configuration.
Direct sites	Pass-through site configuration.
Direct arps	Pass-through arp configuration.
Direct hosts	Authentication-free user configuration.

【Prompt Information】-

【Platform Description】 -

1.42 show web-auth auth-server

Display the basic information of the local http server (for docking with the clearpass server)

show web-auth auth-server

【Parameter Description】

Parameter	Description

-	-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Display the basic information of the local http server

【Configuration Example】

```
AC-FS#sh web-auth auth-server
server status: ON
server ip.....1.1.1.1
server port  : 8082
submit url : http://1.1.1.1:8082/login2
connections  : 0
read timeout : 3
write timeout: 10
wait timeout : 30
statistics:
 expired connections: 0
 request id errors  : 0
```

Field Description:

Field	Description
connections	The number of connections currently maintained between the terminal and the device.
read timeout	The timeout for reading data from the socket is the same as the timeout configured by the http redirect timeout command, the default is 3s.
write timeout	Timeout for writing socket, default 10s.

【Prompt Information】 -

【Platform Description】 -

1.43 show web-auth cgi

Displays the CGI configuration.

show web-auth cgi

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Used to view the CGI configuration of web authentication.

【Configuration Example】1: Display the CGI configuration.

```
AC-FS# show web-auth cgi
Total 0 cgi items:
id-string           url-string
_____________       ____________________________________
```

Field Description

Field	Description
id-string	CGI command corresponding ID.
url-string	CGI command string.

【Prompt Information】-

【Platform Description】 -

1.44 show web-auth control

Displays the authentication controlled configuration.

show web-auth control

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Display the authentication configuration and statistics on the interface.

```
AC-FS(config)#show web-auth control
 Port                    Control  Server Name          Online User Count Vlan Control List
 ----------------------- -------- -------------------- ----------------- ------------------
 GigabitEthernet 0/1     On       <not configured>     0---------------------- 2-17,19
AC-FS(config)#
```

Field Description:

Field	Description
Port	Controlled port name.
Control	Whether the port is open for web authentication.
Server Name	The custom server name on the port, <not configured> means not configured.
Online User Count	Number of online users on the interface.

【Prompt Information】-

【Platform Description】 -

1.45 show web-auth direct-arp

Displays the passthrough ARP range.

show web-auth direct-arp

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Display the configuration of the pass-through website.

```
AC-FS(config)#show web-auth direct-arp
Direct arps:
  Address         Mask
  ---------------- ----------------
  1.1.1.1          255.255.255.255
  2.2.2.2 255.255.255.255 AC-
FS(config)#
```

Field Description:

Field	Description
Address	IP address.
Mask	IP address mask.

【Prompt Information】-

【Platform Description】 -

1.46 show web-auth direct-host

Displays the scope of users who are exempt from web authentication.

show web-auth direct-host

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to view the configuration information of the authentication-free user

【Configuration Example】1: Display users who do not need authentication.

```
AC-FS# show web-auth direct-host
Direct hosts:
  Address          Mask             Port       ARP Binding
  ---------------- ---------------- ---------- -----------
  192.168.0.1..... 255.255.255.255  Gi0/2      On
  192.168.4.11     255.255.255.255  Gi0/10     On
  192.168.5.0      255.255.255.0    Gi0/16     Off
```

Field Description:

Field	Description
Address	There is no need to authenticate the user's IP address.
Mask	There is no need to authenticate the user's IP address mask.
ort	Port of the device bound to the user IP.
ARP Binding	Whether to perform ARP binding

【Prompt Information】-

【Platform Description】 -

1.47 show web-auth direct-site

Displays the pass-through site range.

show web-auth direct-site

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Display the configuration of the pass-through website.

```
AC-FS(config)#show web-auth direct-site
Direct sites:
  Address         Mask            ARP Binding
  ---------------  ---------------  ----------

  1.1.1.1..... 255.255.255.255 Off
  2.2.2.2 255.255.255.255 On AC-
FS(config)#
```

Field Description:

Field	Description
Address	IP address.
Mask	IP address mask.
ARP Binding	Yes Perform ARP binding.

【Prompt Information】-

【Platform Description】 -

1.48 show web-auth global

Display the global WEB authentication configuration information.

show web-auth global

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Used to view the basic Parameter configuration of global web authentication.

【Configuration Example]】1: Display the global WEB authentication configuration information.

```
AC-FS#          show          web-auth          global
Webauth.....enable
Webauth-type.....external
Customized-pages.....(Not Configured)
Server-port.....8081
Public account.....disable
Authentication.....(Not Configured)
Current global template:
    name.....eportalv1
    type.....v1
    Ip:.....192.168.197.79
    URL:.....http://192.168.197.79:8080/eportal/index.jsp
```

Field Description:

Field	Description
Webauth-type	Web authentication type.
Public account	Shared account is enabled.
Authentication	Authentication method.
Current global template	Current global template information.

【Prompt Information】-

【Platform Description】 -

1.49show web-auth global authentication

Displays the global WEB authentication method.

show web-auth global authentication

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Used to view the basic Parameter configuration of web authentication.

【Configuration Example】1: Display the global WEB authentication method.

```
AC-FS#  show  web-auth  global  authentication
Webauth.....enable
Authentication.....(Not Configured)
```

Field Description:

Field	Description
Webauth	WEB authentication is enabled.
Authentication	Authentication method.

【Prompt Information】-

【Platform Description】 -

1.50show web-auth global customized-pages

Display WEB authentication custom page information.

show web-auth global customized-pages

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 It is used to view the information of WEB authentication customized page.

【Configuration Example]】1: Display WEB authentication custom page information.

```
AC-FS#  show  web-auth  global  customized-pages
Webauth.....enable
Customized-pages.....(Not Configured)
```

Field Description:

Field	Description
Webauth	WEB authentication is enabled.
Customized-pages	Customize page information.

【Prompt Information】-

【Platform Description】 -

1.51 show web-auth global local-portal

Displays built-in authentication server information.

show web-auth global local-portal

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Used to view the built-in authentication server information.

【Configuration Example】1: Display the built-in authentication server information.

```
AC-FS#   show   web-auth   global   local-portal
Webauth.....enable
Server-port.....8081
Public account.....disable
```

Field Description:

Field	Description
Webauth	WEB authentication is enabled.
Server-port	The server listens on the port.
Public account	Shared account is enabled.

【Prompt Information】 -

【Platform Description】 -

1.52show web-auth global template

Display global web authentication template information.

show web-auth global template

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Used to view the global web authentication template information.

【Configuration Example]】 1: Display global web authentication template information.

```
AC-FS#    show    web-auth    global    template
Webauth.....enable
Current global template:
    name.....eportalv1
    type.....v1
    Ip:.....192.168.197.79
    URL:.....http://192.168.197.79:8080/eportal/index.jsp
```

Field Description

Field	Description

Webauth	WEB authentication is enabled.
Current global template	Current global template information.

【Prompt Information】 -

【Platform Description】 -

1.53 show web-auth global webauth-type

Displays the global web authentication type.

show web-auth global webauth-type

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Used to view the global web authentication type.

【Configuration Example]】 1: Display the global web authentication type.

```
AC-FS#  show  web-auth  global  webauth-type
Webauth.....enable
Webauth-type.....external
```

Field Description:

Field	Description
Webauth	WEB authentication is enabled.
Webauth-type	WEB authentication type.

【Prompt Information】 -

【Platform Description】 -

1.54 show web-auth info

View the WEB authentication configuration information.

show web-auth info

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Used to view WEB authentication configuration information.

【Configuration Example】1: Display WEB authentication configuration information.

```
AC-FS# show web-auth info
web-auth info:
    Update interval: 180
    User mode: ip
    Portal key: AC-FS
```

Field Description:

Field	Description
Update interval	User information update cycle.
User mode	Bind user mode.
Portal key	Portal communication key.

【Prompt Information】-

【Platform Description】 -

1.55 show web-auth ip-mapping

Display the mapping relationship between configured servers and users

show web-auth ip-mapping

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 No configuration.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】

【Configuration Example]】 1: Configuration mapping relationship.

```
AC-FS(config)#show web-auth ip-mapping
-------------------------------------------------------------------------------
  Name:        iportal
  Ip.....0.0.0.0
  Url:
  Ip-Mapping:
-------------------------------------------------------------------------------
  Name:        eportalv1
  Ip.....172.18.105.9
  Url:         http://172.18.105.9:8080/eportal/index.jsp
  Ip-Mapping:
               1.1.1.0-255.255.255.0             GlobalAC-FS(config)#
```

【Verification】

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -EG products take effect

1.56 show web-auth noise

Display the configured noise reduction Parameter information

show web-auth noise

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 No configuration.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】

【Configuration Example】1: Display noise reduction function:

```
AC-FS#show web-auth noise
Noise Enable:  On
  Aging Timer:    1min
  Hit  Counts:    3
```

【Verification】

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.57 show web-auth parameter

Displays the configuration for HTTP redirection.

show web-auth parameter

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Used to view the basic Parameter configuration of web authentication.

【Configuration Example]】1: Display the configuration of HTTP redirection.

```
AC-FS# show web-auth parameter
  session-limit: 10
  timeout:         5
```

Field Description:

Field	Description
session-limit	Maximum number of HTTP sessions for the same unauthenticated user.
timeout	The timeout for maintaining redirected connections.

【Prompt Information】-

【Platform Description】 -

1.58 show web-auth portal-check

Display the configured portal-check Parameter information

show web-auth portal-check

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 No configuration.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】

【Configuration Example]】 1: Configure the portal-check function:

```
AC-FS#sh web portal-check
Check:         Enable
  Interval:    3s
  Timeout:     5s
  Retransmit:  3
Escape:        Enable
Nokick:        Disable
```

【Verification】

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.59 show web-auth rdport

Displays TCP interception ports.

show web-auth rdport

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Display the TCP interception port configuration.

```
AC-FS#show web-auth rdport
Rd-Port:
80 443
AC-FS#
```

【Prompt Information】-

【Platform Description】 -

1.60 show web-auth syslog ip

Query user's upper and lower records.

show web-auth syslog ip ip-address

【Parameter Description】

Parameter	Description
Ip-address	Query by user's ip.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query the user's online and offline records. Restricted Description: This command does not support the preservation of the original data after hot backup.

【Configuration Example】1: Display user log on and off line.

```
AC-FS#show web-auth syslog ip 192.168.197.35
Address: 192.168.197.35 Core-index 0 Current index 2
Index:            0
 Time:             2015-10-16 20:37:34
 Behavior:         ONLINE
 Mac:              00d0.f822.33e7
 Vid:              101
```

```
Port:            Gi3/1
Timeused:        0d 00:00:00
Flow_up:         0
Flow_down:       0

Index:           1
Time:            2015-10-16 20:42:08
Behavior:        OFFLINE
Mac:             00d0.f822.33e7
Vid:             101
Port:            Gi3/1
Timeused:        0d 00:04:27
Flow_up:         2107872
Flow_down:       2108224
```

Field Description:

Field	Description
Index	Record number
Time	record when it happened
Behavior	Action, representing going online or offline
MAC	user mac
Vid	user vid
Port	user port
Timeused	time online
Flow UP	User upstream traffic
Flow down	User downlink traffic

【Prompt Information】-

【Platform Description】 -

1.61 show web-auth template

Displays the portal server configuration.

show web-auth template

【Parameter Description】

Parameter	Description
-	-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to view server configuration information.

【Configuration Example】1: Display users who do not need authentication.

```
AC-FS#show web-auth template
Webauth Template Settings:
----------------------------------------------------------------------------
  Name:       eportalv1
  Url:        http://17.17.1.21:8080/eportal/index.jsp
  Ip.....17.17.1.21
  BindMode:   ip-mac-mode
  Type:       v1
----------------------------------------------------------------------------
  Name:       eportalv2
  Url:        http://17.17.1.21:8080/eportal/index.jsp
  Ip.....17.17.1.21
  BindMode:   ip-only-mode
  Type:       v2
  Port:       50100
  Acctmlist:
  Authmlist: AC-
FS#
```

Field Description:

Field	Description
Name	template name.
Url	Server home page address.
Ip	Server IP address.
Type	Server type. The first generation portal server is v1, the second generation is v2, and the built-in is intra.

Port	Server protocol message communication port, only the second-generation portal server exists.
Acctmlist	Accounting method list name, only the second generation and built-in authentication exist.
Authmlist	Authentication method list name, only the second generation and built-in authentication exist.

【Prompt Information】 -

【Platform Description】 -

1.62 show web-auth user

Display the online information of all users or specified users, including user IP address, interface, online time and other information.

show web-auth user { all | ip ip-address | mac mac-address | name name-string | session-id num | escape | by-ap ap-name | by-ap-group ap-group-name }

【Parameter Description】

Parameter	Description
ip-address	Specifies the user's IPv4 address.
mac-address	Specifies the user's MAC address.
name-string	specify username.
ap-name	Specifies the name of the ap to which the user belongs.
ap-group-name	Specifies the name of the ap group corresponding to the ap to which the user belongs.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Escape is only supported in the usage scenario of WeChat connected to wifi, used to display escape user entries.

【Configuration Example]】 1: Display the global configuration and statistics of web authentication.

```
AC-FS# show web-auth user all
Current user num :  4, online 2

Address           Online   Time Limit     Time Used    Status  Name
_______________  _______  _____________  _____________  _______  _________

192.168.0.11     On       0d 01:00:00   0d 00:15:10    Active
192.168.0.13     On       0d 01:00:00   0d 00:00:59    Active   111
192.168.0.25     Off      0d 01:00:00   0d 00:00:59    Create
192.168.0.46     Off      0d 01:00:00   0d 01:00:00    Destroy  222

AC-FS# show web-auth user ip 192.168.0.11
Address.....................192.168.0.11
 Mac             :   00d0.f800.2233
 Port            :   Gi0/2
 Online         :   On
```

```
 Time Limit    :   0d 01:00:00
 Time Used     :   0d 00:15:10
 Time Start    :   2009-02-22 20:05:10
 Status         :   Active
```

Field Description:

Field	Description
Address	User's IP address.
Mac	The user's MAC address.
Port	The port of the device the user is connected to.
Online	Whether the user is online.
Time Limit	The user's available time limit, 0 means no limit.
Time Used	The user has been online for a while.
Time Start	The time when the user has passed the authentication and started to go online.
Status	User status, Active indicates that the user is online normally, Create indicates that the user has just been created and the settings have not been completed, and Destroy indicates that the user has just been deleted and the settings have not been cleared yet.
Name	Username, the first-generation authentication user device cannot display the username, the column is empty

【Prompt Information】-

【Platform Description】 -

1.63temporary-permit

Set the temporary release function of WeChat connected to wifi authentication.

temporary-permit seconds

Disable the temporary release function of WeChat connected to wifi authentication.

no temporary-permit

【Parameter Description】

Parameter	Description
seconds	Configure the duration of temporary release. Unit: second, the recommended value is 30s ~ 60s.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Template configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Configure the temporary release function

```
AC-FS(config.tmplt.wechat)# temporary-permit 30
```

【Verification】 Use show web-auth template to view the currently configured template parameter.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.64time-interval

Set the built-in authentication advertisement popup interval.

time-interval { hour }

Restore the default time interval.

no time-interval

【Parameter Description】

Parameter	Description
hour	Ad popup time interval, the default is 1 hour, the value range is 0-24.

【Default Configuration】 The default is 1 hour.

【Command Mode】 Template configuration mode.

【Default Level】 14

【Usage Guide】

【Configuration Example]】1: Configure the pop-up time interval for advertisements to be 2 hours

```
AC-FS(config.tmplt.iportal)#time-interval 2
```

【Verification】Use show web-auth template to view the currently configured template Parameter

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.65url

Set the page address of the portal server.

url url-string

Delete the home page address of the certification page.

no url

【Parameter Description】

Parameter	Description
url-string	The page address should start with "http://" or "https://", otherwise it will prompt that the configuration is unsuccessful, and the maximum length is 255 characters.

【Default Configuration】 By default, the page address of the portal server is not set.

【Command Mode】 Template configuration mode.

【Default Level】 14

【Usage Guide】 This command replaces the original http redirect homepage [url-string] command; the original command is hidden and implemented as a compatible command.

If the url is not configured, the default format will be used: http://[ip-address], where [ip-address] is the server IP address configured by the IP command.

【Configuration Example]】1: Specify the page address of the eportalv1 template as "http://www.web-auth.net/login".

```
AC-FS(config.tmplt.eportalv1)#url http://www.web-auth.net/login
```

【Verification】Use show web-auth template to view the currently configured template Parameter

【Prompt Information】 1. Illegal URL format.

```
%Error: Invalid homepage URL.
```

【Common Mistake】-

【Platform Description】 -

1.66version

Set the version used by WeChat to connect to wifi authentication.

version {1.0 | 16wifi | 3.0 }

Restore the default version that uses WeChat to connect to wifi authentication.

no version

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 Version 11.1(5)B8 uses version 1.0 by default, and version 11.1(5)B9 uses version 3.0 by default.

【Command Mode】 Template configuration mode.

【Default Level】 14

【Usage Guide】 After it is configured as 16wifi, it will support the colorful WeChat scan function.

【Configuration Example]】1: Configure the version that uses WeChat to connect to wifi authentication.

```
AC-FS(config.tmplt.wechat)#version 16wifi
```

【Verification】Use show web-auth template to view the currently configured template parameter.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.67 webauth

Enable web authentication in WLANSEC mode.

webauth

Delete the default configuration.

no webauth

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 It is not enabled by default.

【Command Mode】 WLANSEC configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Enable web authentication under wlansec 1.

```
AC-FS (config)# wlansec 1
AC-FS (config-wlansec)# webauth
```

【Verification】Use show running-config to view the current configuration

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.68 web-auth accounting jitter-off

If the device is configured with anti-shake function or low-traffic offline, this function determines whether to calculate the anti-shake time or low-traffic detection time into the online duration in accounting packets. This function is used to reduce billing errors. If the billing policy in the environment allows these detection times not to be deducted, this function can be configured. If anti-shake or low-traffic detection is configured, by default, the anti-shake time or low-traffic detection time is not included in the online duration.

web-auth accounting jitter-off

Restore default configuration.

no web-auth accounting jitter-off

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 The default is not included.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure anti-shake accounting.

```
AC-FS (config)# web-auth accounting jitter-off
```

【Verification】Use show running-config to view the current configuration

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.69 web-auth accounting v2

Specifies the accounting update method.

web-auth accounting v2 { default | name }

Restore default configuration.

no web-auth accounting v2 { default | name }

【Parameter Description】

Parameter	Description
name	Accounting method name.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Global or template configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the list of accounting methods.

```
AC-FS (config.tmplt.eportalv2)# web-auth accounting v2 default
```

【Verification】Use show running-config to view the current configuration

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.70 web-auth accout-share ip-limit

Use local authentication for built-in and enable the account sharing function. At this time, you can limit the number of users who can log in with the account.

web-auth account-share ip-limit {limit-num}

Delete configuration.

no web-auth account-share

【Parameter Description】

Parameter	Description
Limit-num	Limit the number of online accounts with the same name.

【Default Configuration】 No configuration.

【Command Mode】Config configuration mode

【Default Level】 14

【Usage Guide】

【Configuration Example】1: Configure limit parameter.

```
AC-FS (config)# web-auth account-share ip-limit {limit-num}
```

【Verification】Use show running-config to view the current configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -EG products take effect.

1.71 web-auth authentication v2

Configure the web authentication authentication method.

web-auth authentication v2 [default | name]

Delete configuration.

no web-auth authentication v2 [default | name]

【Parameter Description】

Parameter	Description
name	Specify the web authentication method.

【Default Configuration】 The default method specified by aaa is used by default.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the authentication method.

```
AC-FS (config.tmplt.eportalv2)# web-auth authentication v2 default
```

【Verification】Use show running-config to view the current configuration

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.72 web-auth acl

The whitelist allows users to access some network resources before authentication, and the blacklist prevents users from accessing some network resources after authentication.

web-auth acl { black-ip ip|black-port port | black-url name | white-url name }

Delete configuration.

no web-auth acl { black-ip ip | black-port port | black-url name | white-url name }

【Parameter Description】

Parameter	Description
ip	Blacklist ip addresses.
port	Blacklist port, the value range is 1-65535
name	URLs to blacklist/whitelist.

【Default Configuration】 None.

【Command Mode】 Global configuration mode. Wireless also supports wlansec mode.

【Default Level】 14

【Usage Guide】 -

【Configuration Example]】1: Configure the black and white list.

```
AC-FS (config)# web-auth acl black-ip 192.168.1.2
AC-FS (config)# web-auth acl white-url www.AC-FS.com.cn
```

【Verification】Use show running-config to view the current configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.73 web-auth authen-mode

Web authentication provides IP-based authentication and supports three IP control methods: only IPV4 authentication, only IPV6 authentication, and supports both IPV4 and IPV6 dual stack authentication.

web-auth authen-mode { ipv4 | ipv6 | both }

Restore default configuration.

default web-auth authen-mode

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 Only for IPV4 authentication.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】 If it is configured as both, you need to ensure that ip dhcp snooping is enabled, so that the web authentication component can obtain the IPV6 authentication.

IPV4 address to complete dual-stack authentication.

【Configuration Example】1: Configure the IPV6 authentication mode.

```
AC-FS (config)# web-auth authen-mode ipv6
```

【Verification】Use show running-config to view the current configuration

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.74 web-auth auth-server

Connect to clearpass for web authentication, and configure the relevant parameters of the authentication request packet.

web-auth auth-server { http [port] | ip ip-address | submit-url url-string }

Restore default configuration.

default web-auth auth-server { http | ip | submit-url }

【Parameter Description】

Parameter	Description
port	Specify the destination port of the authentication request message, the default is port 8082.
ip-address	Specifies the destination ip of the authentication request message.
url-string	Specifies the url of the authentication request message.

【Default Configuration】 The default port is 8082.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】 The configured port number needs to be distinguished from the port number of http services such as web network management and built-in portal; the destination IP of the packet cannot be configured as a whitelist or a direct website.

【Configuration Example]】1: Configure the destination port of the authentication request message to be 8083, the destination ip to be 2.2.2.2, and the url to be http://2.2.2.2:8083/login2.html.

```
AC-FS (config)# web-auth auth-server http port 8083 AC-
FS (config)# web-auth auth-server ip 2.2.2.2
AC-FS (config)# web-auth auth-server submit-url http://2.2.2.2:8083/login2.html
```

【Verification】Use show running-config to view the current configuration

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.75 web-auth apply-mapping

Application template mapping method under interface.

web-auth apply-mapping name

Delete configuration.

no web-auth apply-mapping

【Parameter Description】

Parameter	Description
name	Template mapping method.

【Default Configuration】 No configuration.

【Command Mode】 Configure in interface mode.

【Default Level】 14

【Usage Guide】

【Configuration Example]】1: Apply the template mapping method test under the configuration interface gi0/1.

```
AC-FS(config-if-GigabitEthernet 0/1)#web-auth apply-mapping test
```

【Verification】Use show running-config to view the current configuration

【Prompt Information】

【Common Mistake】-

【Platform Description】 -

1.76 web-auth bind-portal

Configure MAC SMS authentication to bind the portal server.

web-auth bind-portal string [type { local-spec | group-spec }]

Delete configuration.

no web-auth bind-portal

【Parameter Description】

Parameter	Description
string	Bind the portal server name.

【Default Configuration】 None.

【Command Mode】 WLANSEC configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure MAC SMS authentication to bind the portal server.

```
AC-FS (wlansec)# web-auth bind-portal eportalv2
```

【Verification】Use show running-config to view the current configuration.

【Prompt Information】-

【Common Mistake】-

1.77 web-auth dhcp-check

Configure the dhcp address verification function for web authentication, and only terminals with addresses assigned through dhcp are allowed to perform authentication.

web-auth dhcp-check

Restore default configuration.

no web-auth dhcp-check

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 Close.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Enable dhcp address verification

```
AC-FS (config)# web-auth dhcp-check
```

【Verification】Use show running-config to view the current configuration

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.78 web-auth direct-host

Set the IP range of users without authentication.

web-auth direct-host { ipv4-address [ip-mask] [arp] | ipv6-address | mac-address} [port interface-name]

Cancel without authenticating the user.

no web-auth direct-host { ipv4-address [ip-mask] | ipv6-address | mac-address}

【Parameter Description】

Parameter	Description
Ipv4-address	There is no need to authenticate the user's IPv4 address.
Ipv6-address	There is no need to authenticate the user's IPv6 address.

ip-mask	(Optional) The IPv4 address mask of the user that does not need to be authenticated.
port interface-name	(Optional) Bind the user IP to the port of the device.
arp	(Optional) If the ARP CHECK function is enabled on the device, ARP binding needs to be performed on the authentication-free user IP range, and the arp keyword needs to be configured. Required only when setting an IPv4 address.
mac-address	No need to authenticate the user's MAC address

【Default Configuration】 By default, no user authentication is required. All users must pass Web authentication before they can access restricted network resources.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】 Set the user as a user without authentication, then the user does not need to perform web authentication, and can also access all reachable network resources. A maximum of 50 unauthenticated user network ranges are allowed.

【Configuration Example]】1: Set the user whose IP address is 172.16.0.1 as a user without authentication.

```
AC-FS(config)# web-auth direct-host 172.16.0.1
```

2: Set the user whose MAC address is 0000:5e00:0101 as a user without authentication.

```
AC-FS(config)# web-auth direct-host 0000:5e00:0101
```

【Verification】Use the show web-auth direct-host command to view the configuration parameter.

【Prompt Information】 1: Illegal IP/mask format

```
%Error: Invalid IP address.
```

【Common Mistake】-

【Platform Description】 -

1.79 web-auth dkey-compatible url-parameter

Set the Ningdun system compatible URL Parameter.

web-auth dkey-compatible url-parameter string

Cancel compatible URLs.

no web-auth dkey-compatible url-parameter

【Parameter Description】

Parameter	Description
string	post parameter field.

【Default Configuration】 There is no configuration by default, which is not compatible with Ningdun system.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】 None.

【Configuration Example】1: Set the post Parameter to login.

```
AC-FS(config)# web-auth dkey-compatible url-parameter login
```

【Verification】Use the show running-config command to view the configuration Parameter.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.80 web-auth enable

Start web authentication on the port. Compatible with the original web-auth port-control command.

web-auth enable [eportalv1 | eportalv2 | template-name]

Turn off web authentication on the port.

no web-auth enable

【Parameter Description】

Parameter	Description

eportalv1	Default Generation Authentication Template.
eportalv2	Default second-generation authentication template.
template-name	custom template name.

【Default Configuration】 By default, Web authentication is disabled on the port.

The eportalv1 template is used by default.

【Command Mode】 Interface configuration mode.

【Default Level】 14

【Usage Guide】 To successfully apply the web authentication function, you must configure the home page address of the authentication page.

Since the application of the template is integrated into the controlled switch, the configuration of the template/server application on the original interface without authentication is automatically cleared. Compatible with the original global application template/server function.

【Configuration Example]】 1: Enable web authentication on port gigabitEthernet 0/14.

```
AC-FS(config)# interface GigabitEthernet 0/14
AC-FS(config-if-GigabitEthernet 0/14)# web-auth enable
```

【Verification】 View the configuration information of the controlled port through show web-auth control.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.81 web-auth group

Configure group information.

web-auth group group-name [description description-str]

Delete configuration.

no web-auth group group-name

【Parameter Description】

Parameter	Description
Group-name	Created group name.
Description-str	Description of the group.

【Default Configuration】-

【Command Mode】Config configuration mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example]】1: Create group information

```
AC-FS (config)# web-auth group group-1 [description DESC]
```

【Verification】Use show running-config to view the current configuration

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.82 web-auth logging enable

Enable the web authentication SYSLOG feature.

web-auth logging enable { num }

Turn this feature off.

no web-auth logging enable

【Parameter Description】

Parameter	Description

num	SYSLOG printing rate, the number of SYSLOG printed per second. Range [0, 65535], 0 means no limit.

【Default Configuration】 The default is to disable the web authentication SYSLOG function.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】 This command only restricts the SYSLOG printed by the module under normal conditions, and the abnormal or serious SYSLOG is not restricted.

【Configuration Example】1: The configuration module SYSLOG prints unlimited speed.

```
AC-FS(config)# web-auth logging enable 0
```

【Verification】View configuration information through show running-config

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.83 web-auth mapping

CONFIGURING THE WEBAUTH TEMPLATE MAPPING METHOD.

web-auth mapping name {vlan vlan-list | ip-mapping ipv4 mask | vxlan vni-list } { template tmplt-name {[dst-ip]} | ssid ssid-str }

Delete configuration.

no web-auth mapping name {vlan [vlan-list] | ip-mapping ipv4 mask | vxlan vni-list }

【Parameter Description】

Parameter	Description
name	Template mapping method.

vlan-list	vlan list.
ipv4	Use the ip network segment of this template.
mask	use the template's ip mask.
tmplt-name	template name.
dst-ip	destination ip.
vni-list	vni list.
ssid-str	SSID Parameter.

【Default Configuration】 No configuration.

【Command Mode】 Configuration mode.

【Default Level】 14

【Usage Guide】 -

【Configuration Example]】1: Configure the mapping method test1 to map the template eportalv2 and vlan 2-5,10.

```
AC-FS (config)# web-auth mapping test1 vlan 2-5,10 template eportalv2
```

1: Configure the mapping method map_test to redirect users on the 10.10.10.1 network segment using the template stu_1.

```
AC-FS(config)#web-auth mapping map_test ip-mapping 10.10.10.1 255.255.255.0 template stu_1
```

【Verification】Use show running-config to view the current configuration

【Prompt Information】

【Common Mistake】-

【Platform Description】 -

1.84 web-auth noise

Configure the wireless web authentication noise reduction policy.

web-auth noise [aging agmin] [hit times]

Restore default configuration.

no web-auth noise

【Parameter Description】

Parameter	Description
agmin	The aging time of the noise table entry, the default is 1 minute, the value range is 1-30.
times	Noise determination rule: access a certain destination ip for times times, it is considered as noise.

【Default Configuration】 Disable the noise reduction function.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the noise reduction strategy.

AC-FS (config)# web-auth noise aging 1 hit 3

【Verification】Use show running-config to view the current configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.85 web-auth offline-detect

Configure the online detection function of authenticated users under wlansec to log off with low traffic or no traffic within a specified time period.

web-auth offline-detect interval interval flow thredshold

Restore the online detection of authenticated users to the default configuration.

default web-auth offline-detect

Disable online detection of authenticated users.

no web-auth offline-detect

【Parameter Description】

Parameter	Description
interval	Traffic detection period, in minutes, the value range is [1, 65535], the default is 15 minutes.
threshold	Flow, unit byte, value range [0, 4294967294], 0 means no flow detection.

【Default Configuration】 15 minutes no traffic detection offline

【Command Mode】 wlansec mode

【Default Level】 14

【Usage Guide】 10.x disables traffic detection under wlansec by default, and uses the global configuration. So after upgrading 11.x, you need to manually close the configuration under wlansec.

【Configuration Example]】1: After configuring wlansec 1, if the user's traffic is less than 5kBytes within 5 minutes, the user will be offline:

```
AC-FS(config)#wlansec 1
AC-FS(config-wlansec)# web-auth offline-detect interval 5 flow 5120
```

【Verification】1: Use the show running command to view the configuration related to the online detection of authenticated users.

【Prompt Information】-

【Common Mistake】-

1.86 web-auth ping

Check if the portal server is available.

web-auth ping [interval minutes] [retry times]

Restore default configuration.

no web-auth ping

【Parameter Description】

Parameter	Description
minutes	Detection period, the default is 1 minute, the value range is 1-65535.
times	The number of timeout retransmissions, the default is 3 times, the value range is 0-65535.

【Default Configuration】 Disable ping detection.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example]】 1: Configure the ping detection period to be 5 minutes and the number of retransmissions to be 4.

```
AC-FS (config)# web-auth ping interval 5 rerty 4
```

【Verification】 Use show running-config to view the current configuration.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.87 web-auth portal

Specifies the Portal server used for authentication.

web-auth portal { eportalv1 | eportalv2 | iportal | wechat | wifidog | name }

Delete configuration.

no web-auth portal { eportalv1 | eportalv2 | iportal | wechat | wifidog | name }

【Parameter Description】

Parameter	Description
name	The specified template name.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the Portal server used for specified authentication:

```
AC-FS(config)# web-auth portal eportalv2
```

【Verification】Use show running-config to view the current configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.88 web-auth portal extension

By switching this function on, the FS Portal server and the Portal server of the standard mobile specification can be supported.

no web-auth portal extension

Restore default configuration.

default web-auth portal extension

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 The Ruijie Portal server url format is used by default.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Disable the Portal protocol extension.

```
AC-FS (config)# no web-auth portal extension
AC-FS (config)# http redirect url-fmt ext1
```

【Verification】Use show running-config to view the current configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.89 web-auth portal key

Set the key for communication between the device and the authentication server.

web-auth portal key key-string

Clear the key for communicating with the authentication server after the user's HTTP WEB request is redirected to a new WEB request.

no web-auth portal key

【Parameter Description】

Parameter	Description
key-string	The key for communication between the device and the authentication server, with a maximum length of 255 characters.

【Default Configuration】 By default, no key is set.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】 To successfully apply the Web authentication function, the key for communication between the device and the authentication server must be set. The current server key only supports global configuration and does not support specifying a key for each individual server.

【Configuration Example]】1: Set the key for communication between the device and the authentication server to be web-auth.

```
AC-FS(config)# web-auth portal key web-auth
```

【Verification】View server key configuration through show running-config.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.90 web-auth portal-attribute

Configure the transparent transmission function of the 0x05 attribute of the Portal protocol.

web-auth portal-attribute [5 | textinfo]

Restore default configuration.

no web-auth portal-attribute [5 | textinfo]

【Parameter Description】

Parameter	Description
key-string	-

【Default Configuration】 Not configured.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】 Generally, web-auth portal-attribute 5 is enabled when a specific Portal Server (the mobile portal protocol specification in use) requires a device to upload an error ID (ErrID).

Or the Portal Server (using the Huawei portal2.0 protocol specification) requires the device to upload the Prompt Information of a third-party authentication device such as RADIUS.

(TextInfo), enable web-auth portal-attribute textinfo.

【Configuration Example]】1: Configure the transparent transmission function of Portal protocol 0x05 attribute.

```
AC-FS (config)# web-auth portal-attribute 5
or:
AC-FS (config)# web-auth portal-attribute textinfo
```

【Verification】Use show running-config to view the current configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.91 web-auth portal-check

Check if the portal server is available.

web-auth portal-check [interval intsec] [timeout tosec] [retransmit retires]

Restore default configuration.

no web-auth porta-check

【Parameter Description】

Parameter	Description
intsec	Detection period, the default is 10 seconds, the value range is 1-1000.
tosec	Packet timeout, the default is 5 seconds, the value range is 1-1000.
retries	The number of retransmissions over time, the default is 3 times, the value range is 1-100.

【Default Configuration】 Disable portal detection.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】 In most network environments, there is only one server, and this function does not need to be configured. If there are multiple servers, the Parameter should not be set too small, otherwise the device will send too many packets in a short time, which will affect the device performance.

【Configuration Example]】1: Configure portal detection.

```
AC-FS (config)# web-auth portal-check interval 20 timeout 2 retransmit 2
```

【Verification】Use show running-config to view the current configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.92 web-auth portal-escape

Configure portal escape. When the configured portal server is unavailable, users who newly access the network are exempt from authentication.

web-auth portal-escape

Restore default configuration.

no web-auth portal-escape

【Parameter Description】

Parameter	Description

【Default Configuration】 Close.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】 If there are some key services in the network that cannot be interrupted, you can configure this function, so that when the Portal server is abnormal, the services can be guaranteed not to be affected. To configure this function, you need to configure the Portal detection function at the same time.

【Configuration Example]】1: Configure portal escape.

```
AC-FS (config)# web-auth portal-escape
```

【Verification】Use show running-config to view the current configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.93 web-auth portal-valid unique-name

Configure the uniqueness check function of the Portal authentication account.

web-auth portal-valid unique-name

Restore default configuration.

no web-auth portal-vallid unique-name

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 Not configured.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】 Generally, it is enabled when Portal Server needs to push "terminal preemption" Prompt Information to users.

【Configuration Example]】1: Configure the uniqueness check function of the Portal authentication account.

```
AC-FS (config)# web-auth portal-valid unique-name
```

【Verification】Use show running-config to view the current configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.94 web-auth sms-flow

Configure the free traffic period and threshold for MAC SMS authentication.

web-auth sms-flow [interval interval] [I threshold flows]

Delete configuration.

no web-auth sms-flow [interval interval] [I threshold flows]

【Parameter Description】

Parameter	Description
interval	Detection cycle, in minutes.
flows	Inspect traffic, in KB.

【Default Configuration】 Not configured.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Configure the mac SMS detection threshold.

```
AC-FS (config)# web-auth sms-flow interval 5 flows 100
```

【Verification】Use show running-config to view the current configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.95 web-auth sta-leave detection

Configure to disable link detection. After the terminal passes the web authentication, the link is disconnected, and the authentication entry will not be deleted. When the terminal connects to the network again, as long as the IP address is the same as the previous one, it can continue to surf the Internet.

no web-auth sta-leave detection

Restore default configuration.

default web-auth sta-leave detection

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 Not closed.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Disable link detection.

```
AC-FS (config)# no web-auth sta-leave detection
```

【Verification】Use show running-config to view the current configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.96 web-auth sta-perception enable

Configure the command to enable the non-sensing function of WeChat authentication.

web-auth sta-perception enable

Delete configuration.

no web-auth sta-perception enable

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 No configuration.

【Command Mode】 Global configuration mode or wireless WLAN security mode

【Default Level】 14

【Usage Guide】

【Configuration Example]】 1: Configure the command to enable the WeChat authentication non-sensing function.

```
AC-FS# web-auth sta-perception enable
```

【Verification】Use show running-config to view the current configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.97 web-auth template

Create and enter the default generation authentication template configuration mode.

web-auth template eportalv1

Create and enter custom generation authentication template configuration mode.

web-auth template { template-name } v1

Create and enter the default second-generation authentication template configuration mode.

web-auth template eportalv2

Create and enter the custom second-generation authentication template configuration mode.

web-auth template { template-name } v2

Create and enter the default built-in authentication template configuration mode.

web-auth template iportal

Create and enter custom built-in authentication template configuration mode.

web-auth template { template-name } intra

Create and enter the default wifidog template configuration mode.

web-auth template wifidog

Create and enter custom wifidog template configuration mode.

web-auth template { template-name } wifidog

Create and enter the default WeChat connection wifi authentication template configuration mode.

web-auth template wechat

Create and enter the custom WeChat connection wifi authentication template configuration mode.

web-auth template { template-name } wechat

To delete a template use the following command.

no web-auth template { template-name }

【Parameter Description】

Parameter	Description
eportalv1	Default generation authentication template.
eportalv2	Default second-generation authentication template.

iportal	Default built-in authentication template.
wechat	Default WeChat connection wifi authentication template.
wifidog	Default wifidog authentication template.
template-name	Custom authentication template name.

【Default Configuration】 Serverless configuration

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】 Enter the eportalv1 template mode to configure ip and url to replace the original http redirect and http redirect homepage commands. At the same time, the device needs to be compatible with the original http redirect and http redirect homepage command configuration methods, and the internal automatic conversion to this Command format.
Compatible with the original portal-server command configuration, and automatically converted to the new command.
To successfully apply the web authentication function, an available portal server must be configured and applied; the default eportalv1 template will be applied by the system by default; the eportalv1 template usually contains the IP address, url and communication key that need to be set, if the url is not configured The default format will be used: http://[ip-address]. The IP address of the portal server is also an authentication-free network resource. Unauthenticated users can also access it. However, in order to prevent attacks, the device restricts the upstream traffic of users accessing this IP. The specific upper limit of the limit value is related to the number of physical ports on the device. proportional.

【Configuration Example]】 1: Configure the eportalv1 template.

```
AC-FS(config)# web-auth template eportalv1
AC-FS(config.tmplt.eportalv1)#
```

【Verification】 Use show web-auth template to view the currently configured template.

【Prompt Information】 1. It is not allowed to change the template type.

```
%Notice: Template has been created, it is a v2 template.
```

【Common Mistake】 -

【Platform Description】 -

1.98 web-auth update-interval

Configure the online user update interval.

web-auth update-interval {seconds}

Restore default configuration.

no web-auth update-interval

【Parameter Description】

Parameter	Description
seconds	Information update interval, in seconds. The value range is 30-3600. The default is 180 seconds.

【Default Configuration】 180 seconds.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】 1: Set the update interval of authenticated user information to 60 seconds.

```
AC-FS (config)# web-auth update-interval 60
```

【Verification】Use show running-config to view the current configuration

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.99 web-auth valid-ip-acct

Configure the time allowed to wait for the user to obtain an IP address. If the user does not obtain an IP address after this time, the user will be kicked offline.

web-auth valid-ip-acct [timeout seconds]

Restore default configuration.

no web-auth valid-ip-acct

【Parameter Description】

Parameter	Description
seconds	The time allowed to wait for the user to obtain an IP, in seconds, the default is 30 seconds.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This configuration takes effect only for unaware users who are connected to wifi by WeChat.

【Configuration Example]】1: Configure the time allowed to wait for the user to obtain an IP to be 1 minute.

```
AC-FS(config)# web-auth valid-ip-acct timeout 60
```

【Verification】Use show running-config to view the current configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.100 web-auth wechat-check

Configure the server detection function of WeChat connected to wifi authentication.

web-auth wechat-check interval minutes

Disable server detection.

no web-auth wechat-check

【Parameter Description】

Parameter	Description
minutes	Escape time interval, it is recommended to configure it to 30 minutes.

【Default Configuration】 No configuration.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】 The server detection function only takes effect when the collective escape function is enabled (refer to the escape command).

【Configuration Example】1: Configure the server detection function parameter.

```
AC-FS (config)# web-auth wechat-check interval 30
```

【Verification】Use show running-config to view the current configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.101 web-auth wechat-escape

Configure the collective escape function of WeChat connected to wifi authentication.

web-auth wechat-escape interval minutes times count

Turn off the collective escape function.

no web-auth wechat-escape

Cancel the collective escape state and restore the individual escape state. It is a trigger command, and show running-config does not display it.

web-auth wechat-escape recover

【Parameter Description】

Parameter	Description
minutes	Escape interval, default 60 minutes.
count	The number of consecutive escape users, the default is 5.

【Default Configuration】 No configuration.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 The collective escape function needs to be enabled only when the individual escape function (refer to the escape command) is enabled.

【Configuration Example]】1: Configure the collective escape function detection Parameter.

```
AC-FS (config)# web-auth wechat-escape interval 30 times 10
```

【Verification】Use show running-config to view the current configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.102 web-auth wechat-template wlan-range portal-ip nas-ip

Configure wireless WeChat to wifi one-key configuration.

web-auth wechat-template name wlan-range wlanid-start wlanid-end portal-ip portal-ip-addr nas-ip

nas-ip-addr [nas-id nas-id-str] [ios-adapter | perception]

Delete wireless WeChat connection wifi one-key configuration.

no web-auth wechat-template name

【Parameter Description】

Parameter	Description

name	template name.
wlanid-start	controlled wlan start.
wlanid-end	controlled wlan end.
portal-ip-addr	the address of the portal server.
nas-ip-addr	Set the device access service ip of WeChat connected to wifi, which is used for the server to initiate communication to this ip.
nas-id-str	Device nas-id Parameter, hot standby and VAC scenarios must be configured, otherwise multiple devices cannot be externally reflected as one device.
ios-adapter	Configure the automatic pop-up function.
perception	Configure the senseless function.

【Default Configuration】 No configuration.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Before starting the one-click configuration, wlansec must be created first, otherwise the wlansec that has not been created cannot be configured successfully.

The nas-id configuration is only applicable to hot standby and VAC scenarios, and no configuration is required for single-machine scenarios.

【Configuration Example】Configure one-key configuration for wireless WeChat connection to wifi.

```
AC-FS(config)# web-auth wechat-template aaa wlan-range 1 32portal-ip 172.21.6.78 nas-ip
192.168.197.227
```

【Verification】Use show running-config to view the current configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.103 web-auth wifidog-template wlan-range portal-ip nas-ip url

Configure wireless wifidog one-click configuration.

web-auth wifidog-template name wlan-range wlanid-start wlanid-end portal-ip portal-ip-addr nas-ip nas-ip-addr url url-string [gateway-id gwid-str] [perception]

Delete wireless wifidog one-click configuration.

no web-auth wifidog-template name

【Parameter Description】

Parameter	Description
name	template name.
wlanid-start	controlled wlan start.
wlanid-end	controlled wlan end.
portal-ip-addr	the address of the portal server.
nas-ip-addr	Set the device access service ip of wifidog for the server to initiate communication to this ip.
url-string	The address of the authentication page of the portal server.
gwid-str	Device serial number, in hot standby and VAC scenarios, multiple devices are externally reflected as one device, and this Parameter must be configured.
perception	Configure the senseless function.

【Default Configuration】 No configuration.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Before starting the one-click configuration, you must create a wlansec, otherwise the wlansec that has not been created cannot be configured successfully.

The gateway-id configuration is only applicable to the hot standby and VAC scenarios, and does not need to be configured in the single-server scenario.

【Configuration Example】Configure wireless wifidog one-key configuration.

```
AC-FS(config)# web-auth wifidog-template aaa wlan-range 1 32 portal-ip 172.21.6.78 nas-ip
192.168.197.227 url http://172.21.6.78/auth/wifidogAuth
```

【Verification】Use show running-config to view the current configuration

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.104 web-auth wlan-ac-ip

Configure the ACIP parameters in the redirAect URL.

web-auth wlan-ac-ip ipv4

Delete configuration.

no web-auth wlan-ac-ip

【Parameter Description】

Parameter	Description
ipv4	ACIP Parameter Fields.

【Default Level】No configuration.

【Command Mode】 WLANSEC configuration mode

【Default Level】14

【Usage Guide】 -

【Configuration Examples】 Configure the ACIP parameter in the redirect URL.

```
AC-FS (wlansec)# web-auth wlan-ac-ip 192.168.1.100
```

【Verification】 Use show running-config to view the current configuration

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.105 web-auth winterface

Configure the winterface parameter in the redirect URL.

web-auth winterface string

Delete Configuration.

no web-auth winterface

【Parameter Description】

Parameter	Description
string	winterface Parameter Fields.

【Default Configuration】 No configuration.

【Command Mode】 WLANSEC configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Examples】 1: Configure the winterface parameter.

```
AC-FS (wlansec)# web-auth winterface winterface
```

【Verification】 Use show running-config to view the current configuration

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

2 AAA

2.1 aaa accounting commands

Keeps an accounting of command activity performed by users logged on to the NAS and manages user activity.

aaa accounting commands level { default | list-name } start-stop method1 [method2...]

Cancel the command bookkeeping function.

no aaa accounting commands level { default | list-name }

【Parameter Description】

Parameter	Description
level	The command level to be booked, ranging from 0 to 15, determines which level of command execution is required to record the information message.
default	If this parameter is used, the list of methods defined later is used as the default method for command bookkeeping.
list-name	Define a list of command bookkeeping methods, which can be any string.
method	One of the keywords listed in "none, group" is required, and a method list can have up to 4 methods:
none	Do not do bookkeeping.
group	Use server groups for bookkeeping, currently TACACS+ server groups are supported.

【Default Configuration】 Bookkeeping function off

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 FSOS will enable the command accounting function only after the user has passed the login authentication. If the user is not authenticated when logging in or the authentication method is none, command accounting will not be performed. If the user is not authenticated when logging in or the authentication method is none, no accounting will be performed. When the accounting function is enabled, after each user executes a specified level of command, the information of the executed command will be sent to the security server. After the command accounting method is configured, it must be applied to the terminal line that needs to perform command accounting, otherwise it will not take effect.

【Configuration Examples】 The following example uses TACACS+ to perform accounting for command requests executed by users, and the command level required for accounting is level 15.

```
AC-FS(config)# aaa accounting commands 15 default start-stop group tacacs+
```

【Verification】 Use the show aaa method-list command to view the information of the configured command accounting method list.

【Prompt Information】 1: If the specified group is not defined on the device, an error is prompted.

```
:%Group XXX is not existed
```

2: If the group type does not support this bookkeeping type, an error will be prompted.

```
The accounting does not support this type of group
```

3: If this command is configured repeatedly, the new configuration overwrites the original configuration.

【Common Mistake】 -

【Platform Description】

2.2 aaa accounting exec

To manage user activity by accounting for user access activities when logged into the NAS.

aaa accounting exec { default | list-name } start-stop method1 [method2...]

Cancel the Exec accounting function.

no aaa accounting exec { default | list-name }

【Parameter Description】

Parameter	Description
default	With this parameter, the list of methods defined later is used as the default method for Exec bookkeeping.
list-name	Defines a list of methods for Exec bookkeeping, which can be any string.
method	It must be one of the keywords listed in "none, group", a method list can have up to 4 methods：
none	No accounting.

group	Use server groups for accounting, currently RADIUS and TACACS+ server groups are supported.

【Default Configuration】 Turn off the accounting function.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 FSOS will enable the Exec accounting function only after the user has passed the login authentication. If the user is not authenticated when logging in or the authentication method is none, the Exec accounting will not be performed.

After the accounting function is enabled, when the user logs in to the CLI interface of the NAS, the accounting start (Start) message is sent to the security server, and when the user logs out, the accounting end (Stop) message is sent to the security server. If a user logs in without issuing a Start message, it also does not issue a Stop message when logging out.

After configuring the Exec accounting method, it must be applied to the terminal line that needs to perform command accounting, otherwise it will not take effect.

【Configuration Examples】 The following example uses RADIUS to account for user logins to the NAS, and sends accounting messages at the beginning and end.

```
AC-FS(config)# aaa accounting exec default start-stop group radius
```

【Verification】 Use the show aaa method-list command to view the information of the configured Exec accounting method lis.

【Prompt Information】 1: If the specified group is not defined on the device, an error will be displayed.

```
%Group XXX is not existed
```

2: If the group type does not support this type of accounting, then an error is prompted.

```
The accounting does not support this type of group
```

3: If this command is configured repeatedly, the new configuration overrides the original configuration.

【Common Mistake】 -

【Platform Description】 -

2.3 aaa accounting network

For network expense accounting or to manage user activity, you need to account for user access activity.

aaa accounting network { default | list-name } start-stop method1 [method2...]

Cancel the network accounting function.

no aaa accounting network { default | list-name }

【Parameter Description】

Parameter	Description
default	If this Parameter is used, the list of methods defined later is used as the default method for Network bookkeeping.
list-name	The name of the bookkeeping method list.
start-stop	A bookkeeping message is sent at the beginning and end of user access activity, and the start bookkeeping message allows the user to start network access regardless of whether or not bookkeeping is successfully.
method	Enables bookkeeping, allowing the user to begin network access.
none	No bookkeeping.
group	Use server groups for bookkeeping, currently RADIUS and TACACS+ server groups are supported.

【Default Configuration】 Close the bookkeeping function

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 FSOS keeps track of incoming user activity by sending logging attributes to the security server. Use the keyword start-stop to set user accounting options.

【Configuration Examples】 The following example uses RADIUS to account for user requests for network services and sends accounting messages at the beginning and end of the process.

```
AC-FS(config)# aaa accounting network default start-stop group radius
```

【Verification】 Use the show aaa method-list command to view the information of the configured network accounting method list.

【Prompt Information】 1: If the specified group is not defined on the device, an error is prompted.

```
%Group XXX is not existed
```

2: If the group type does not support this type of accounting, then an error is prompted.

The accounting does not support this type of group

3: If this command is configured repeatedly, the new configuration overwrites the original configuration.

【Common Mistake】 -

【Platform Description】 -

2.4 aaa accounting update

Enables the accounting update feature, which is used to enable global accounting updates.

aaa accounting update

Disables the accounting update function.

no aaa accounting update

【Parameter Description】 -

【Default Configuration】 Disable the accounting update function by default.

【Command Mode】 Global mode.

【Default Level】 14

【Usage Guide】 If the AAA security service is not enabled, the accounting update cannot be used. If the AAA security service is enabled, this command is used to set the bookkeeping update function.

【Configuration Examples】 The following example demonstrates setting up the accounting update enablement.

```
AC-FS(config)# aaa new-model
AC-FS(config)# aaa accounting update
```

【Verification】 Use the show aaa accounting update command to see if the accounting update function is enabled.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

2.5 aaa accounting update periodic

Set the accounting update interval for the accounting update feature that has been enabled.

aaa accounting update periodic interval

Configure the default accounting update interval.

no aaa accounting update periodic

【Parameter Description】

Parameter	Description
interval	Bookkeeping update interval, in minutes, with a minimum of 1 minute.

【Default Configuration】 5 minutes

【Command Mode】 Global mode.

【Default Level】 14

【Usage Guide】 If AAA security service is not enabled, you cannot use accounting update. If the AAA security service is enabled, this command is used to set the bookkeeping update interval.

【Configuration Examples】 1: The following example demonstrates setting up the bookkeeping update every 1 minute.

```
AC-FS(config)# aaa new-model AC-FS(config)# aaa accounting update
AC-FS(config)# aaa accounting update periodic 1
```

【Verification】 Use the show aaa accounting update command to view the configuration information of the accounting update interval.

【Prompt Information】 If this command is repeatedly configured, the new configuration overrides the original configuration.

【Common Mistake】 -

【Platform Description】 -

2.6 aaa authentication dot1x

To use AAA for 802.1X user authentication, execute the global configuration command aaa authentication dot1x to configure the 802.1X user authentication method list.

aaa authentication dot1x { default | list-name } method1 [method2...]

Deletes the list of methods for 802.1X user authentication.

No aaa authentication dot1x { default | list-name }

【Parameter Description】

Parameter	Description
default	Using this Parameter, the list of methods defined later is used as the default method for 802.1X user authentication.
list-name	Define a list of methods for 802.1X user authentication, which can be any string.
method	It must be one of the keywords listed as "local, none, group", and a method list can have up to 4 Method.
local	Use local username database for authentication.
none	No authentication.

【Default Configuration】 -

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】If the device enables the AAA 802.1X security service, users must use AAA for 802.1X user authentication negotiation. You must use the aaa authentication dot1x command to configure the default or optional list of methods for 802.1X user authentication.

【Configuration Examples 】 The following example defines a list of AAA 802.1X user authentication methods named rds_d1x. This list of authentication methods first uses the RADIUS security server for authentication, and if no response is received from the RADIUS security server within a certain time frame, the local user database is used for authentication.

```
AC-FS(config)# aaa authentication dot1x rds_d1x group radius local
```

【Verification】Use the show aaa method-list command to view the information of the configured 802.1X authentication method list.

【Prompt Information】 1: If the specified group is not defined on the device, an error will be prompted.

%Group XXX is not existed

2: If the group type does not support this authentication type, an error will be prompted.

The authentication does not support this type of group

3: If this command is configured repeatedly, the new configuration overwrites the original configuration.

【Common Mistake】 -

【Platform Description】 -

2.7 aaa authentication enable

To use AAA for enable authentication, execute the global configuration command AAA Authentication enable to configure the method list of enable authentication.

aaa authentication enable default method1 [method2...]

Delete the list of authentication methods.

no aaa authentication enable default

【Parameter Description】

Parameter	Description
default	If this Parameter is used, the method list defined later is used as the default method for Enable authentication. Enable authentication is based on global authentication, and currently only supports setting the default authentication method list.
method	Must be one of the keywords listed in "local, none, group, enable", a method list has a maximum of 4 methods.
local	Authenticate using a local username database.
none	Not authenticated.
group	Authentication using server groups, currently supports RADIUS and TACACS+ server groups.

【Default Configuration】 -

【Command Mode】 Global mode.

【Default Level】 14

【Usage Guide】If the device enables the AAA Enable authentication service, users must use AAA for Enable authentication negotiation. You must use the aaa authentication enable command to configure the default list of methods for Enable authentication.

Only if there is no response from the previous methods can the later methods be used for authentication.

Enable authentication method list is configured.

【Configuration Examples】 The following example defines a list of AAA Enable authentication methods. This list of authentication methods first uses the RADIUS security server for authentication, and if no answer is received from the RADIUS security server within a certain time frame, the local user database is used for authentication.

```
AC-FS(config)# aaa authentication enable default group radius local
```

【Verification】 Use the show aaa method-list command to view the information of the configured Enable authentication method list.

【Prompt Information】

1: If the specified group is not defined on the device, an error is prompted.

```
%Group XXX is not existed
```

2: If the group type does not support this type of authentication, an error will be displayed.

```
The authentication does not support this type of group.
```

3: If this command is configured repeatedly, the new configuration overwrites the original configuration.

【Common Mistake】 -

【Platform Description】 -

2.8 aaa authentication iportal

To use AAA for device-built Portal Web user authentication, execute the global configuration command aaa authentication iportal to configure the list of methods for device-built Portal Web user authentication.

aaa authentication iportal { default | list-name } method1 [method2...]

Deletes the list of authentication methods.

no aaa authentication iportal { default | list-name }

【Parameter Description】

Parameter	Description
Default	If this Parameter is used, the method list defined later is used as the default method for the built-in Portal Web user authentication of the device.
list-name	Defines a list of methods for the device's built-in Portal Web user authentication, which can be any string.
method	Must be one of the keywords listed in "local, none, group, subs", a method list has a maximum of 4 methods.
local	Authenticate using a local username database.
none	no authentication.
group	Use server groups for authentication, currently RADIUS server groups are supported.

【Default Configuration】 -

【Command Mode】 Global mode

【Default Level】14

【Usage Guide】 If the appliance enables the AAA appliance built-in Portal Web security service, users must use AAA for appliance built-in Portal Web user authentication negotiation. You must use the aaa authentication iportal command to configure the default or optional list of methods for appliance built-in Portal Web user authentication.

Only if there is no response from the previous methods can the later methods be used for authentication.

【Configuration Examples】 The following example defines a list of built-in Portal Web authentication methods for AAA devices named rds web. This list of authentication methods first uses the RADIUS security server for authentication, and if no answer is received from the RADIUS, security server within a certain time frame, the local user database is used for authentication.

```
AC-FS(config)# aaa authentication iportal rds_web group radius local
```

【Verification】 Use the show aaa method-list command to view the information of the configured iportal authentication method list.

【Prompt Information】 1: If the specified group is not defined on the device, an error is prompted.

```
%Group XXX is not existed
```

2: If the group type does not support this type of authentication, an error is prompted.

```
The authentication does not support this type of group
```

3: If this command is configured repeatedly, the new configuration overwrites the original configuration.

【Common Mistake】 -

【Platform Description】

2.9 aaa authentication login

To use AAA for Login authentication, execute the global configuration command aaa authentication login to configure the list of methods for Login authentication.

aaa authentication login { default | list-name } method1 [method2...]

Delete the list of authentication methods.

no aaa authentication login { default | list-name }

【Parameter Description】

Parameter	Description
default	Using this Parameter, the list of methods defined later is used as the default method for Login authentication.
list-name	Define a list of methods for Login authentication, which can be any string.
method	It must be one of the keywords listed as "local, none, group, subs", and a method list can have up to 4 Methods.
local	Use local username database for authentication.
none	No authentication.
group	Authentication using server groups, currently RADIUS and TACACS+ server groups are supported.
subs	Use the subs database for authentication.

【Default Configuration】 -

【Command Mode】 Global mode.

【Default Level】 14

【Usage Guide】 If the device enables AAA login authentication security service, users must use AAA for Login authentication negotiation. You must use the aaa authentication login command to configure the default or optional list of methods for Login authentication.

Only if there is no response from the previous method can the later method be used for authentication.

After setting the Login authentication method, you must apply it to the terminal line that requires Login authentication, otherwise it will

not take effect.

【 Configuration Examples 】 The following example defines a list of AAA Login authentication methods named list-1. The authentication method list first uses the RADIUS security server for authentication, and if no answer is received from the RADIUS security server within a certain time frame, the local user database is used for authentication.

```
AC-FS(config)# aaa authentication login list-1 group radius local
```

【Verification】 Use the show aaa method-list command to view the information of the configured Login authentication method list.

【Prompt Information】 1: If the specified group is not defined on the device, an error is prompted.

```
%Group XXX is not existed
```

2: If the group type does not support this type of authentication, an error will be displayed.

```
The authentication does not support this type of group.
```

3: If this command is configured repeatedly, the new configuration overwrites the original configuration.

【Common Mistake】 -

【Platform Description】 -

2.10 aaa authentication ppp

To use AAA for PPP user authentication, execute the global configuration command aaa authentication ppp to configure the list of methods for PPP user authentication.

aaa authentication ppp { default | list-name } method1 [method2...]

Delete the list of authentication methods.

no aaa authentication ppp { default | list-name }

【Parameter Description】

Parameter	Description
default	Using this Parameter, the list of methods defined later is used as the default method for PPP user authentication.

list-name	Define a list of methods for PPP user authentication, which can be any string.
method	It must be one of the keywords listed in "local, none, group, subs", and a method list can have up to There are 4 methods.
local	Use local username database for authentication.
none	No authentication.
group	Use server group for authentication, currently RADIUS server group is supported.
subs	Use the subs database for authentication.

【Default Configuration】 -

【Command Mode】 Global mode.

【Default Level】 14

【Usage Guide】 If the device enables the AAA PPP security service, the user must use AAA for PPP user authentication negotiation. You must use the aaa authentication ppp command to configure a list of default or optional methods for PPP user authentication.
The latter method can be used for authentication only if the former method does not respond.

【Configuration Example】: 1: The following example defines a list of AAA PPP authentication methods named rds_ppp. The authentication method list uses the RADIUS security server for authentication first, and if no response is received from the RADIUS security server within a certain time limit, the local user database is used for authentication.

```
AC-FS(config)# aaa authentication ppp rds_ppp group radius local
```

【Verification】 Use the show aaa method-list command to view the list of configured PPP authentication methods.

【Prompt Information】 1: If the specified group is not defined on the device, it will prompt an error.

```
%Group XXX is not existed
```

2: If the group type does not support this authentication type, an error will be prompted.

```
The authentication does not support this type of group
```

3: If this command is configured repeatedly, the new configuration will overwrite the original configuration.

【Common Mistake】 -

【Platform Description】 -

2.11 aaa authentication sslvpn

To use AAA for sslvpn user authentication, execute the global configuration command aaa authentication sslvpn to configure the list of methods for sslvpn user authentication.

aaa authentication sslvpn { default | list-name } method1 [method2...]

Deletes the list of methods for sslvpn user authentication.

no aaa authentication sslvpn { default | list-name }

【Parameter Description】

Parameter	Description
default	Using this Parameter, the list of methods defined later is used as the default method for sslvpn user authentication.
list-name	Define a list of methods for sslvpn user authentication, which can be any string.
method	It must be one of the keywords listed as "local, none, group, subs", and a method list can have up to There are 4 methods.
local	Use local username database for authentication.
none	No authentication.
group	Use server group for authentication, currently RADIUS server group is supported.
subs	Use the subs database for authentication.

【Default Configuration】 -

【Command Mode】 Global mode.

【Default Level】 14

【Usage Guide】 If the device enables the sslvpn service, users must use AAA for sslvpn user authentication negotiation. You must use the aaa authentication sslvpn command to configure the default or optional list of methods for sslvpn user authentication.

Only if there is no response from the previous method can you use the later method for authentication.

【Configuration Examples】 The following example defines a list of AAA sslvpn user authentication methods called rds sslvpn. This list of authentication methods first uses the RADIUS security server for authentication and then uses the local user database for authentication if no answer is received from the RADIUS security server within a certain time frame.

```
AC-FS(config)# aaa authentication sslvpn rds_sslvpn group radius local
```

【Verification】 Use the show aaa method-list command to view the information of the configured sslvpn authentication method list.

【Prompt Information】 1: If the specified group is not defined on the device, an error will be prompted.

```
%Group XXX is not existed
```

2: If the group type does not support this type of authentication, an error is prompted.

```
The authentication does not support this type of group
```

3: If this command is configured repeatedly, the new configuration overwrites the original configuration.

【Common Mistake】 -

【Platform Description】 -

2.12 aaa authentication web-auth

To use AAA for second-generation Web authentication, execute the global configuration command aaa authentication.

web-auth to configure the list of methods for second-generation Web authentication for the device. aa authentication web-auth { default | list-name } method1 [method2...]

Delete the list of authentication methods.

no aaa authentication web-auth { default | list-name }

【Parameter Description】

Parameter	Description
default	Using this Parameter, the list of methods defined later is used as the default method for Device 2 Web Authentication.
list-name	Define a list of methods for Device 2 Web Authentication, which can be any string.
method	It must be one of the keywords listed in "local, none, group, subs", and a method list can have up to There are 4 methods.
local	Use local username database for authentication.
none	No authentication
group	Use server group for authentication, currently RADIUS server group is supported.

【Default Configuration】 -

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 If the appliance enables the AAA Appliance II Web Security Service, users must use AAA for appliance II Web user authentication negotiation. You must use the aaa authentication web-auth command to configure the default or optional list of methods for Device 2 Web user authentication.

Only if there is no response from the previous method can you use the later method for authentication.

【Configuration Examples】 1: The following example defines a list of AAA device second-generation Web authentication methods named rds_web. The authentication method list first uses the RADIUS security server for authentication, and if no answer is received from the RADIUS security server within a certain time frame, it is released directly and the authentication passes.

```
AC-FS(config)# aaa authentication web-auth rds_web group radius none
```

【Verification】 Use the show aaa method-list command to view the information of the configured web-auth authentication method list.

【Prompt Information】 1: If the specified group is not defined on the device, an error will be prompted.

```
%Group XXX is not existed
```

2: If the group type does not support this type of authentication, an error is prompted.

```
The authentication does not support this type of group.
```

3: If this command is configured repeatedly, the new configuration overwrites the original configuration.

【Common Mistake】 -

【Platform Description】 -

2.13 aaa authorization commands

For users who have logged on to the CLI interface of the NAS, use the AAA command authorization feature to authorize commands executed by the user, allowing or disallowing a user to execute specific commands. Execute the global configuration command aaa authorization commands.

aaa authorization commands level { default | list-name } method1 [method2...]

Disables the AAA command authorization feature.

no aaa authorization commands level { default | list-name }

【Parameter Description】

Parameter	Description
level	The command level to be authorized, ranging from 0 to 15, determines which level of command needs to be authorized before to be executed.
default	If this Parameter is used, the list of methods defined later is used as the default method for command authorization.
list-name	Define a list of methods for command authorization, which can be any string.
method	It must be one of the keywords listed in "none, group", and a method list can have up to 4 methods.
none	No authorization.
group	Use server groups for authorization, currently TACACS+ server groups are supported.

【Default Configuration】 Disable the AAA command authorization function.

【Command Mode】 Global mode.

【Default Level】 14

【Usage Guide】 FSOS supports authorization of user-executable commands. When a user enters and tries to execute a command, AAA sends the command to the security server, and if the security server allows the command to be executed, the command is executed, otherwise the command is not executed and a prompt is given that the execution of the command is rejected.

When configuring command authorization, you need to specify the level of the command, which is the default level of the command (for example, if a command is visible to users of level 14 or higher, the default level of the command is level 14). After configuring the command authorization method, you must apply it to the terminal line that needs command authorization, otherwise it will not take effect.

【Configuration Examples】 1: The following example uses the TACACS+ server to authorize level 15 commands.

```
AC-FS(config)# aaa authorization commands 15 default group tacacs+
```

【Verification】 Use the show aaa method-list command to view the information of the configured command authorization method list.

【Prompt Information】 1: If the specified group is not defined on the device, an error will be displayed.

```
%Group XXX is not existed
```

2: If the group type does not support this type of authorization, an error is displayed.

The authorization does not support this type of group.

3: If this command is configured repeatedly, the new configuration overwrites the original configuration.

【Common Mistake】 -

【Platform Description】 -

2.14 aaa authorization config-commands

To use AAA to authorize commands in configuration mode (including global configuration mode and its submodes), execute the global configuration command aaa authorization config-commands.

aaa authorization config-commands

Disables the ability of AAA to authorize commands in configuration mode.

no aaa authorization config-commands

【Parameter Description】 -

【Default Configuration】 Disables AAA authorization of commands in configuration mode.

【Command Mode】 Global mode.

【Default Level】 14

【Usage Guide】 If you only authorize the commands in non-configuration mode (such as privileged mode), you can use the no mode of this command to turn off the authorization function of configuration mode, then the commands in configuration mode and its sub-mode can be executed without command authorization.

【Configuration Examples 】 1: The following example turns on the authorization function for commands in configuration mode.

AC-FS(config)# aaa authorization config-commands

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

2.15 aaa authorization console

To use AAA to authorize commands executed by users who log in through the console, execute the global configuration command aaa authorization console.

aaa authorization console

Disables AAA authorization of commands executed by users logging in through the console.

no aaa authorization console

【Parameter Description】 -

【Default Configuration】 Disables the authorization function of AAA for commands executed by users logged in through the console.

【Command Mode】 Global mode.

【Default Level】 14

【Usage Guide】 FSOS supports the distinction between users logged in through the console and those logged in through other terminals, and you can set whether command authorization is required for users logged in through the console. If the command authorization function of the console is disabled, the command authorization method list that has been applied to the console line will not take effect.

【Configuration Examples】 The following example configures the command authorization function for console login users.

```
AC-FS(config)# aaa authorization console
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

2.16 aaa authorization exec

To use AAA to grant Exec authorization to users logged into the CLI interface of the NAS with a privilege level, execute the global configuration command aaa authorization exec.

aaa authorization exec { default | list-name } method1 [method2...]

Disable the authorization feature of AAA Exec.

no aaa authorization exec { default | list-name }

【Parameter Description】

Parameter	Description
default	Using this Parameter, the list of methods defined later is used as the default method for Exec authorization.
list-name	Define a list of Exec-authorized methods, which can be any string.
method	It must be one of the keywords listed in "local, none, group", and a method list can have up to 4 methods.
local	Use local username database for authorization.
none	No authorization.
group	Use server groups for authorization, currently RADIUS and TACACS+ server groups are supported.

【Default Configuration】 Disables the AAA Exec authorization feature.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 FSOS supports the authorization of users who log in to the CLI interface of the NAS, giving them CLI privilege levels (0~15). Currently, Exec authorization is performed only for users who have passed Login authentication. If the Exec authorization fails, the CLI interface cannot be accessed. After you configure the Exec authorization method, you must apply it to the terminal line that requires Exec authorization, otherwise it will not take effect.

【Configuration Examples】 The following example uses a RADIUS server for Exec authorization.

```
AC-FS(config)# aaa authorization exec default group radius
```

【Verification】 Use the show aaa method-list command to view information about the configured Exec authorization method list.

【Prompt Information】 1: If the specified group is not defined on the device, an error is prompted.

```
%Group XXX is not existed
```

2: If the group type does not support this type of authorization, then an error is prompted.

```
The authorization does not support this type of group
```

3: If this command is configured repeatedly, the new configuration overwrites the original configuration.

【Common Mistake】 -

【Platform Description】 -

2.17 aaa authorization network

To use AAA to authorize service requests to access network users (including protocols such as PPP, SLIP, and so on), execute the global configuration command aaa authorization network.

aaa authorization network { default | list-name } method1 [method2...]

Disables the authorization function of AAA.

no aaa authorization network { default | list-name }

【Parameter Description】

Parameter	Description
default	When this Parameter is used, the list of methods defined later is used as the default method for Network authorization.
method	Must be one of the keywords listed in "none, group", a method list can have up to 4 methods.
none	No network authorization.
group	Use server groups for authorization, currently RADIUS and TACACS+ server groups are supported.

【Default Configuration】 Disable the AAA Network authorization feature.

【Command Mode】 Global mode.

【Default Level】 14

【Usage Guide】 FSOS supports authorization for all network-related service requests such as PPP, SLIP, and other protocols. If authorization is configured, authorization is automatically performed for all authenticated users or interfaces.

Three different authorization methods can be specified. As with authentication, only if there is no response from the current authorization method can authorization continue using the subsequent methods, and if the current authorization method fails, no other subsequent authorization methods will be used.

The RADIUS or TACACS+ server completes authorization of the authenticated user by returning a series of attribute pairs. Therefore, network authorization is based on authentication, and it is only possible to obtain network authorization if the authentication is passed.

【Configuration Examples】 The following example uses a RADIUS server to authorize a network service.

```
AC-FS(config)# aaa authorization network default group radius
```

【Verification】 Use the show aaa method-list command to view the information of the configured Network authorization method list.

【Prompt Information】 1: If the specified group is not defined on the device, an error is prompted.

```
%Group XXX is not existed
```

2: If the group type does not support this type of authorization, an error will be displayed.

```
The authorization does not support this type of group
```

3: If this command is configured repeatedly, the new configuration overwrites the original configuration.

【Common Mistake】 -

【Platform Description】 -

2.18 aaa domain

Enter the domain configuration mode and configure the properties of the domain.

aaa domain { default | domain-name }

Cancel this command.

no aaa domain { default | domain-name }

【Parameter Description】

Parameter	Description
default	Use this Parameter to configure the default domain.
domain-name	Specifies the name of the domain.

【Default Configuration】 No domain is configured.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Default is the default domain configuration, which is the list of methods used by the network device if the user does not carry the domain information. domain-name is the specified domain configuration, which specifies the list of methods associated with this domain if the user carries the domain name. The system currently supports a maximum of 32 domains.

【Configuration Examples】 The following example demonstrates setting up a domain name configuration.

```
AC-FS(config)# aaa domain AC-FS.com
AC-FS(config-aaa-domain)#
```

【Verification】 Use show aaa domain command to view the domain configuration information.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

2.19 aaa domain enable

The general domain-based AAA service switch, which is off by default. When this switch is turned on, all AAA services take precedence over the domain-based AAA service configuration.

aaa domain enable

Disables this switch.

no aaa domain enable

【Parameter Description】 -

【Default Configuration】 The domain name-based AAA service switch is disabled.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 To configure AAA service based on domain name, you need to open this configuration switch.

【Configuration Example]】1: Turn on the domain name-based AAA service switch:

```
AC-FS(config)# aaa domain enable
```

【Verification】Use the show aaa domain command to view the domain configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.20 aaa heartbeat enable

The AAA heartbeat detection switch, which is on by default. When this switch is turned on, the AAA process and the AAA library detect the availability of the counterpart by heartbeat signals.

aaa heartbeat enable

Disables this switch.

no aaa heartbeat enable

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 AAA Heartbeat detection is on.

【Command Mode】 Global mode.

【Default Level】 14

【Usage Guide】 This feature is enabled by default, but only known AAA front-end modules support heartbeat (such as radius, dot1x, etc.).

【Configuration Examples 】 1: Disable the AAA heartbeat detection function.

```
AC-FS(config)# no aaa heartbeat enable
```

【Verification】 Use the show run command to view the domain configuration information.

【Prompt Information】-

【Common Mistake】 -

【Platform Description】 -

2.21 aaa local authentication attempts

Configure the number of failed login attempts for login users.

aaa local authentication attempts max-attempts

【Parameter Description】

Parameter	Description
max-attempts	The maximum number of failed attempts, ranging from 1 to 2147483647.

【Default Configuration】 The default value is 3 times.

【Command Mode】 Global mode.

【Default Level】 14

【Usage Guide】 This command configures the number of failed login attempts for Login users.

【Configuration Examples】 Configure the number of failed login attempts for Login users to 6 times.

```
AC-FS# configure terminal
AC-FS(config)# aaa local authentication attempts 6
```

【Verification】 Use the show aaa lockout command to view lockout configuration information.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

2.22 aaa local authentication lockout-time

Configure the length of time that a login user is locked out after exceeding the configured number of failed login attempts.

aaa local authentication lockout-time lockout-time

【Parameter Description】

Parameter	Description
lockout-time	Lock time (unit: minutes), the value range 1~2147483647.

【Default Configuration】 The default value is 15 minutes.

【Command Mode】 Global mode.

【Default Level】 14

【Usage Guide】 Configure the length of time that the Login login user is locked out after exceeding the configured number of failed login attempts.

【Configuration Examples】 Configure the length of time the Login user is locked out after exceeding the configured number of failed login attempts to 5 minutes.

```
AC-FS# configure terminal
AC-FS(config)# aaa local authentication lockout-time 5
```

【Verification】 Use the show aaa lockout command to view the lockout configuration information.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

2.23 aaa local user allow public account

Configure whether the local account (username or subs) can be shared by more than one terminal in case of Web authentication.

aaa local user allow public account

【Parameter Description】 -

【Default Configuration】 Off, which means that a local account is not allowed to be shared by multiple endpoints.

【Command Mode】 Global mode.

【Default Level】 14

【Usage Guide】 This configuration is only supported on EG series products, and other products support local accounts being shared by multiple terminals by deft.

【Configuration Examples】 Configure the number of failed login attempts for Login users to 6.

```
AC-FS#configure terminal
AC-FS(config)#aaa local user allow public account
```

【Verification】 Use the show run command to view the configuration information.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 This configuration is only supported on EG series products, and other products support local accounts being shared by multiple terminals by default.

2.24 aaa log enable

To print the syslog of AAA user authentication, execute the aaa log enable command to turn on the switch.

aaa log enable

Do not print the syslog of AAA user authentication.

no aaa log enable

【Parameter Description】

Parameter	Description
-	-

【Default Configuration】 Prints the syslog of AAA user authentication.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Print the syslog of AAA user authentication when a large number of users are online, which may cause screen scrubbing or performance degradation of the device, so you can disable the printing function by configuring this command.

【Configuration Examples】 1: The following example closes the syslog that prints the authenticated aaa user.

```
AC-FS(config)# no aaa log enable
```

【Verification】 Use the show running-config command to see if the print aaa user authentication via syslog feature is enabled.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

2.25 aaa log rate-limit

To adjust the print rate of the syslog passed by AAA user authentication, execute the aaa log rate-limit command to configure it.

aaa log rate-limit num

Restores the default print rate for syslogs authenticated by AAA users.

no aaa log rate

【Parameter Description】

Parameter	Description
num	The number of syslogs to be printed per second, ranging from 0 to 65535: 0: no limit on the printing rate. 1 - 65535: Configurable print rate range, the default value is 5.

【Default Configuration】 5, i.e., 5 syslogs per second of AAA user authentication passed.

【Command Mode】 Global mode.

【Default Level】 14

【Usage Guide】 Print the syslog of AAA user authentication when a large number of users are online, which may cause screen scrubbing or performance degradation of the device. Therefore, you can configure this command to adjust the printing rate of the syslogs authenticated by users.

【Configuration Examples】 The following example adjusts the printing rate of the AAA user-authenticated syslog to 10 syslogs per second.

```
AC-FS(config)# aaa log rate-limit 10
```

【Verification】 Use the show running-config command to view the print rate of the syslog authenticated by the AAA user.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

2.26 aaa new-model

To use the AAA security service feature of RGOS, execute the global configuration command aaa new-model to enable AAA.

aaa new-model

Disables the AAA security service.

no aaa new-model

【Parameter Description】 -

【Default Configuration】 Disables the AAA security service.

【Command Mode】 Global mode.

【Default Level】 14

【Usage Guide】 If you want to use AAA security service, you must use aaa new-model to enable AAA security service. If AAA is not enabled, all AAA commands will not be configurable.

【Configuration Examples】 The following example enables the AAA security service.

```
AC-FS(config)# aaa new-model
```

【Verification】 Use the show running-config command to see if the AAA security service is enabled.

【Prompt Information】

【Common Mistake】 -

【Platform Description】

2.27 access-limit

Set the user limit of the domain, only valid for IEEE802.1x users.

access-limit num

Remove the restriction on the number of domain users.

no access-limit

【Parameter Description】

Parameter	Description
num	Limit the number of domain users to IEEE802.1x users only.

【Default Configuration】 By default, the number of users is not limited.

【Command Mode】 Domain configuration mode.

【Default Level】 14

【Usage Guide】 Use this command to limit the number of users in the domain.

【Configuration Example]】1: The following example demonstrates setting the number of users in the domain whose domain name is AC-FS.com to 20.

```
AC-FS(config)# aaa domain AC-FS.com
AC-FS(config-aaa-domain)# access-limit 20
```

【Verification】Use the show aaa domain command to view the configuration information of the user limit of the domain.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.28accounting network

Configure the Network accounting list in domain configuration mode.

accounting network { default | list-name }

Cancel the order.

no accounting network

【Parameter Description】

Parameter	Description
default	Use this Parameter to specify the use of the Default Configuration method list.

list-name	Specify the name of the method list.

【Default Configuration】 When no method list is specified, if a user initiates a request, the network device will try to specify the default method list for the user.

【Command Mode】 Domain configuration mode.

【Default Level】 14

【Usage Guide】Specifies a list of Network accounting methods to use for the domain.

【Configuration Example]】1: The following example demonstrates the list of accounting methods specified in the Network setting field:

```
AC-FS(config)# aaa domain AC-FS.com
AC-FS(config-aaa-domain)# accounting network default
```

【 Verification 】 Use the show aaa domain command to view the configuration information of the network accounting method list specified by the domain.

【Prompt Information】 1: If the specified method list name exceeds the length limit, an error will be prompted.

```
Method list name is too long
```

2: If the specified method list has not been configured, an error will be prompted.

```
%WARNING: method list named XXX for this type is not existed
```

3: If this command is configured repeatedly, the new configuration will overwrite the original configuration.

【Common Mistake】-

【Platform Description】 -

2.29authentication dot1x

Configure the IEEE802.1x authentication list in domain configuration mode.

authentication dot1x { default | list-name }

Cancel the order.

no authentication dot1x

【Parameter Description】

Parameter	Description
default	Use this Parameter to specify the use of the Default Configuration method list.
list-name	Specify the name of the method list.

【Default Configuration】 When no method list is specified, if a user initiates a request, the network device will try to specify the default method list for the user.

【Command Mode】 Domain configuration mode.

【Default Level】 14

【Usage Guide】Specify a list of 802.1x authentication methods for the domain.

【Configuration Example]】1: The following example demonstrates the list of 802.1x authentication methods specified in the setting domain:

```
AC-FS(config)# aaa domain AC-FS.com
AC-FS(config-aaa-domain)# authentication dot1x default
```

【Verification】 Use the show aaa domain command to view the configuration information of the 802.1x authentication method list specified by the domain.

【Prompt Information】 1: If the specified method list name exceeds the length limit, an error will be prompted.

```
Method list name is too long
```

2: If the specified method list has not been configured, an error will be prompted.

```
%WARNING: method list named XXX for this type is not existed
```

3: If this command is configured repeatedly, the new configuration will overwrite the original configuration.

【Common Mistake】-

【Platform Description】 -

2.30authorization network

Configure the Network authorization list in domain configuration mode.

authorization network { default | list-name }

Cancel the order.

no authorization network

【Parameter Description】

Parameter	Description
default	Use this Parameter to specify the use of the Default Configuration method list.
list-name	Specify the name of the method list.

【Default Configuration】 When no method list is specified, if a user initiates a request, the network device will try to specify the default method list for the user.

【Command Mode】 Domain configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example】】 1: The following example demonstrates setting the domain to specify the list of Network authorization methods:

```
AC-FS(config)# aaa domain AC-FS.com
AC-FS(config-aaa-domain)# authorization network default
```

【Verification】 Use the show aaa domain command to view the configuration information of the network authorization method list specified by the domain.

【Prompt Information】 1: If the specified method list name exceeds the length limit, an error will be prompted.

```
Method list name is too long
```

2: If the specified method list has not been configured, an error will be prompted.

%WARNING: method list named XXX for this type is not existed

3: If this command is configured repeatedly, the new configuration will overwrite the original configuration.

【Common Mistake】-

【Platform Description】 -

2.31 clear aaa local user lockout

Clear the locked user list.

clear aaa local user lockout { all | user-name word }

【Parameter Description】

Parameter	Description
all	Indicates all locked out users.
user-name word	Specify the locked out user ID.

【Command Mode】 Privileged mode.

【Default Level】 14

【Usage Guide】 Clear the locked user list, you can clear all or specific users.

【Configuration Example】1: Clear all locked users.

AC-FS# clear aaa local user lockout all

【Prompt Information】 1: If a specified user is cleared and the user exists, then Prompt Information.

User XXX unlocked

【Platform Description】 -

2.32show aaa accounting update

Displays information about accounting updates.

show aaa accounting update

【Parameter Description】 -

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】 14

【Usage Guide】 Displays information related to accounting update, including whether the accounting update switch is turned on and the accounting update interval information.

【Configuration Example】1: Display information about accounting update

```
AC-FS# show aaa accounting update
```

【Prompt Information】-

【Platform Description】 -

2.33 show aaa domain

Displays information about all currently configured domains.

show aaa domain [default | domain-name]

【Parameter Description】

Parameter	Description
default	Use this Parameter to specify the default domain information to be displayed.
domain-name	Show domain information for the specified domain.

【Command Mode】 Privileged mode, global mode, interface mode.

【Default Level】 14

【Usage Guide】 If no domain name is specified, all domain information will be displayed.

【Configuration Example]】 1: The following example displays the domain information of the specified domain name domain.com.

```
AC-FS# show aaa domain domain.com

=============Domain domain.com=============
State: Active
Username format: Without-domain
Access limit: No limit
802.1X Access statistic: 0
```

```
Selected method list:
 authentication dot1x default
```

【Prompt Information】-

【Platform Description】 -

2.34 show aaa lockout

Displays the lock configuration parameters of the current login.

show aaa lockout

【Parameter Description】 -

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】 14

【Usage Guide】 This command displays the lock configuration parameters of the current login.

【Configuration Example]】1: Display the lock configuration of the current login

```
AC-FS# show aaa lockout
Lock tries:  3
Lock timeout:  15 minutes
```

【Prompt Information】-

【Platform Description】 -

2.35show aaa group

Displays all server groups configured for AAA.

show aaa group

【Parameter Description】 -

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】 14

【Usage Guide】 This command displays all the configured server groups of AAA.

【Configuration Example]】 1: Display all configured server groups of AAA.

```
AC-FS# show aaa group
Type       Reference  Name
---------- ---------- ----------
radius   1   radius   tacacs+           1
tacacs+
radius     1          dot1x_group
radius     1          login_group
radius     1          enable_group
```

【Prompt Information】-

【Platform Description】 -

2.36 show aaa method-list

Displays a list of all AAA methods.

show aaa method-list

【Parameter Description】-

【Command Mode】 Privileged mode, global mode, interface mode.

【Default Level】 14

【Usage Guide】 This command displays a list of all methods of AAA.

【Configuration Example]】1: The following example displays a list of AAA methods.

```
AC-FS# show aaa method-list
Authentication method-list
aaa authentication login default group radius
aaa authentication ppp default group radius
aaa authentication dot1x default group radius
aaa authentication dot1x san-f local  group angel group rain none
aaa authentication enable default group radius
Accounting method-list
aaa accounting network default start-stop group radius
Authorization method-list
aaa authorizating network default group radius
```

【Prompt Information】-

【Platform Description】 -

2.37 show aaa user

Display information about aaa users.

show aaa user { all | lockout | by-id session-id | by-name user-name }

【Parameter Description】

Parameter	Description
all	View all AAA user information.
lockout	View information about the list of AAA users that are currently locked.
by-id session-id	View information about AAA users with the specified session id.
by-name user-name	View information about the AAA user with the specified username.

【Command Mode】 Privileged mode, global mode, interface mode.

【Default Level】 14

【Usage Guide】 Display AAA user related information.

【Configuration Example]】1: The following example displays information about AAA users

```
AC-FS#show aaa user all

      Id---------- Name
2345687901        wwxy


AC-FS# show aaa user by-id 2345687901

      Id---------- Name
2345687901        wwxy

AC-FS# show aaa user by-name wwxy
```

```
AC-FS# show aaa user lockout

Name                                Tries       Lock        Timeout(min)
---------------------------------- ---------- ---------- ------------

AC-FS#
```

【Prompt Information】-

【Platform Description】 -

2.38state

Set whether the domain is valid.

state { block | active }

Restore to default configuration.

no state

【Parameter Description】

Parameter	Description
block	Configured domains are valid.
active	The configured domain is not valid.

【Default Configuration】 By default, the domain is valid.

【Command Mode】 Domain configuration mode.

【Default Level】 14

【Usage Guide】 Specify whether the configured domain is valid.

【Configuration Example]】 1: The following example demonstrates that the setting field is invalid.

```
AC-FS(config)# aaa domain AC-FS.com
AC-FS(config-aaa-domain)# state block
```

【Verification】Use the show aaa domain command to check whether the domain is valid.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.39 username-format

Configure whether to carry domain information in the username when the NAS interacts with the server in domain configuration mode.

username-format { without-domain | with-domain }

Restore to default configuration.

no username-format

【Parameter Description】

Parameter	Description
without-domain	Strip domain information.
with-domain	No stripping of domain information

【Default Configuration】 By default, domain information is not stripped.

【Command Mode】 Domain configuration mode.

【Default Level】 14

【Usage Guide】 In the domain configuration mode, configure whether the user name carries domain information when the NAS interacts with the server for the specified domain.

【Configuration Example]】1: The following example demonstrates setting stripped domain information:

```
AC-FS(config)# aaa domain AC-FS.com
AC-FS(config-aaa-domain)# username-domain without-domain
```

【Verification】Use the show aaa domain command to check whether the domain carries the domain name information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3 RADIUS

3.1aaa group server radius

Enter the AAA server group configuration mode.

aaa group server radius name

Delete the server group.

no aaa group server radius name

【Parameter Description】

Parameter	Description
name	The server group name cannot currently be the keywords "radius", "tacacs+", as these are the default server group names for RADIUS and TACACS+ are the default server group names.

【Default Configuration】-

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】 This command configures the AAA server group of RADIUS type.

【Configuration Example]】1: The following example configures a RADIUS-type AAA server group with the group name ss.

```
AC-FS(config)# aaa group server radius ss
AC-FS(config-gs-radius)# end
AC-FS# show aaa group
Type       Reference  Name
---------- ---------- ----------
radius    1    radius    tacacs+            1
tacacs+
radius     1          ss
```

【Verification】Use the command show running-config to view the source address interface configuration information of radius packets

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.2ip radius source-interface

Specifies the source address of RADIUS packets.

ip radius source-interface interface-name

Delete the specified RADIUS packet source address.

no radius source-interface interface-name

【Parameter Description】

Parameter	Description
interface-name	Source address interface for radius messages.

【Default Configuration】 The source address of the default radius packet is set by the network layer.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 In order to reduce the workload of maintaining a large amount of nas information on the radius server, you can use this command to set the source address of radius packets. This command will use the first ip address of the specified interface as the source address of the radius packet. This command is used on Layer 3 devices. If the specified interface is in a certain vrf domain, the route of this vrf domain is used for pathfinding when sending packets.

【Configuration Example]】1: Specify the radius packet to obtain the ip address from the FastEthernet 0/0 interface as the source address of the radius packet:.

```
AC-FS(config)# ip radius source-interface fastEthernet 0/0
```

【Verification】Use the command show running-config to view the source address interface configuration information of radius packets

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.3ip vrf forwarding

Select vrf for AAA server group.

ip vrf forwarding vrf_name

remove vrf no ip vrf forwarding selected by AAA server group.

vrf_name vrf name

【Parameter Description】

Parameter	Description
vrf_name	vrf name.

【Default Configuration】

-

【Command Mode】Server group configuration mode.

【Default Level】 14

【Usage Guide】 Select vrf for the specified server group.

【Configuration Example]】 1: The following example selects vrf as vrf_name for the server group ss.

```
AC-FS(config)# aaa group server radius ss AC-
FS(config-gs-radius)# server 192.168.4.12 AC-
FS(config-gs-radius)# server 192.168.4.13 AC-
FS(config-gs-radius)# ip vrf forwarding vrf_name
AC-FS(config-gs-radius)# end
```

【Verification】Use the show radius group command to view the vrf configuration information of the RADIUS server group.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.4radius attribute

Configure the private property type value.

radius attribute { id | down-rate-limit | dscp | mac-limit | up-rate-limit } vendor-type type

Restore the default private property type value.

no radius attribute { id | down-rate-limit | dscp | mac-limit | up-rate-limit } vendor-type

【Parameter Description】

Parameter	Description
id	function id <1-255>
type	Private property type <1-255>

【Default Configuration】 Only identify the default configuration for our company's private properties:

id	Function	Type
1	max down-rate	1
2	q s	2
3	user ip	3
4	vlan id	4
5	ersion to client	5
6	net ip	6
7	user name	7
8	password	8
9	file-directory	9
10	file-count	10
11	file-nam -0	11
2	file-name-	12
13	file-name-2	13
14	file-name-3	14
15	fil -name-4	15
16	max up-rate	16

17	version to server	17
18	flux-max-high32	18
19	flux-max-low32	19
20	proxy-avoid	20
21	dailup-avoid	21
22	ip privilege	22
23	login privilege	42

Expansion:

id	Function	Type
1	ma down-rate	76
2	qos	77
3	user ip	3
4	vlan id	4
5	version to client	5
6	net ip	6
7	user name	7
8	password	8
9	file-directory	9
10	file-count	10
11	file-name-0	11
12	file-name-1	12
13	file-name-2	13
14	file-name-3	14
15	fi e-name-	15
16	max up-rate	75
17	version to server	17
18	flux-max-high32	18
19	flux-max-low32	19
20	proxy-avoid	20
21	dailup-avoid	21
22	ip privilege	22

23	login privilege	42
24	limit to user number	50

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Use this command to configure the private attribute type value to suit different application situations.

【Configuration Example]】1: Define the max up-rate type value as 211.

```
AC-FS(config)# radius attribute 16 vendor-type 211
```

【Verification】Use show radius vendor-specific to view the configuration of private attribute type values.

【Prompt Information】 1: If the configured id is not within the predefined range, an error will be prompted.

```
no application for the id
```

2: If the type value is already used by other properties, an error is displayed

```
the vendor type had allocated by XXXX
```

【Common Mistake】-

【Platform Description】 -

3.5radius vendor-specific extend

Set radius to resolve packets without distinguishing private vendor id

radius vendor-specific extend

Restore to only identify our company's private vendor id

no radius vendor-specific extend

【Parameter Description】-

【Default Configuration】 Only identify our company's private vendor id

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Use this command to identify all vendor id attributes by type according to the configuration.

【Configuration Example]】1: Configure radius to resolve private attributes without distinguishing private vendor ids.

AC-FS(config)# radius vendor-specific extend

【Verification】Use show running-config to check whether the configuration of this command takes effect.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.6radius vendor-specific attribute support

Configure radius to support parsing Cisco, Huawei, and Microsoft private attributes in packets.

radius vendor-specific attribute support { cisco | huawei | ms}

Configuring radius does not support parsing Cisco, Huawei, and Microsoft private attributes in packets

no radius vendor-specific attribute support { cisco | huawei | ms}

【Parameter Description】

Parameter	Description
cisco	Cisco Private Attributes.
huawei	Huawei Private Attributes.
ms	Microsoft Private Properties.

【Default Configuration】 Supports parsing Cisco, Huawei, and Microsoft private attributes in packets.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Use this command to configure whether to support the parsing of Cisco, Huawei, and Microsoft private attributes in packets.

【Configuration Example]】 1: Configure radius to support the resolution of Huawei private attributes in packets.

```
AC-FS(config)# radius vendor-specific attribute support huawei
```

2: Configuring radius does not support Huawei private attributes in parsing packets.

```
AC-FS(config)# no radius vendor-specific attribute support huawei
```

【Verification】Use show running-config to check whether the configuration of this command takes effect. Support parsing is Default Configuration not displayed, show running-config

You can view which manufacturers' unsupported resolutions are configured.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.7radius-server account update retransmit

Configure the function of retransmitting accounting update packets of second-generation Web authentication users.

radius-server account update retransmit

Restore the default configuration for retransmission of accounting update packets.

no radius-server account update retransmit

【Parameter Description】 -

【Default Configuration】 Default Configuration does not retransmit accounting update messages.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Configure the function of retransmitting accounting update packets of second-generation Web authentication users. By

default, retransmission is not performed. This configuration does not affect other types of users.

【 **Configuration Example** 】 1: Configure the function of retransmitting accounting update packets of second-generation Web authentication users.

```
AC-FS(config)#radius-server account update retransmit
```

【**Verification**】Use the command show running-config to view the configuration.

【**Prompt Information**】-

【**Common Mistake**】-

【**Platform Description**】 -

3.8radius-server attribute 31

Specifies the format of the RADIUS Calling-Station-ID attribute (MAC-based).

radius-server attribute 31 mac format { ietf | normal | unformatted }

Restore default RADIUS Calling-Station-ID attribute (MAC-based) format

no radius-server attribute 31 mac format

【**Parameter Description**】

Parameter	Description
ietf	Specify the standard format specified by the ETF (RFC3580), using '-' as a separator. Such as00-D0-F8-33-22-AC.
normal	Specify the common format for representing MAC addresses (dotted hexadecimal format), using '.' as a separator. For example: 00d0.f833.22ac.
unformatted	Specify no format, without any separator, this format is used by default. Example: 00d0f83322ac.

【**Default Configuration**】 Use unformatted format

【**Command Mode**】 Global mode

【**Default Level**】 14

【Usage Guide】 Some RADIUS security servers (mainly used for 802.1x authentication) may only recognize the IETF format. The Calling-Station-ID property is set to IETF format type.

【Configuration Example]】1: The following example defines the RADIUS Calling-Station-ID attribute in IETF format.

```
AC-FS(config)# radius-server attribute 31 mac format ietf
```

【Verification】 Use show running-config to view the format setting information of radius assembly mac.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.9radius-server attribute class

Configure the parsing method of the Class attribute of RADIUS:

radius-server attribute class user-flow-control { format-16bytes | format-32bytes }

Turn off parsing of the RADIUS Class attribute:

no radius-server attribute class user-flow-control

【Parameter Description】

Parameter	Description
user-flow-control	Configure the speed limit configuration to be parsed from the class attribute.
format-16bytes	Configure the format of the speed limit value in the class attribute to be 16 bytes.
format-32bytes	Configure the speed limit value in the class attribute to be in 32-byte format.

【Default Configuration】 By default, the speed limit is not parsed from the class attribute.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 If the server sends the rate limit value through the Class attribute, you need to configure this command.

【Configuration Example]】1: Enable the function of parsing the speed limit configuration from the Class attribute, and the parsing format is 32 bytes.

```
AC-FS(config)#radius-server attribute class user-flow-control format-32bytes
```

【Verification】Use show running-config to view the radius configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.10radius-server dead-criteria

Configure the criteria by which the device determines that the RADIUS security server is unreachable.

radius-server dead-criteria { time seconds [tries number] | tries number }

Restore the standard for the device to determine that the RADIUS security server is unreachable to the default value

no radius-server dead-criteria { time seconds [tries number] | tries number }

【Parameter Description】

Parameter	Description
time seconds	Configure the time condition parameter. If the equipment does not receive the correct response message from the radius security server within the specified time, it is considered that the radius security server meets the unreachable time condition. The range of values set is 1-120 seconds.
tries number	Configure the request continuous timeout condition parameter. When the number of consecutive timeout times of the request message sent by the device to the same radius security server reaches the set number, the radius security server is considered. The condition of unreachable consecutive timeout times is met. The range of settable values is 1-100.

【Default Configuration】 The default value of time seconds is 60 seconds.

The default value of tries number is 10 times.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 If a RADIUS security server satisfies both the time condition and the consecutive request timeout times, the device considers the RADIUS security server unreachable. Using this command, the user can adjust the parameters of the time condition and the number of consecutive timeouts of the request.

【Configuration Example]】1: The following example specifies a duration of 120 seconds, and the number of consecutive timeouts is 20.

```
AC-FS(config)# radius-server dead-criteria time 120 tries 20
```

【Verification】Use show radius parameter to view the standard configuration information that the device determines that the RADIUS security server is unreachable.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.11radius-server deadtime

Sets the length of time for the device to stop sending request packets to the RADIUS security server in the unreachable state.

radius-server deadtime minutes

The length of time that the recovery device stops sending request packets to the RADIUS security server in the unreachable state is the default value.

no radius-server deadtime

【Parameter Description】

Parameter	Description
minutes	Configure the time, in minutes, for the device to stop sending requests to a RADIUS security server that is in the unreachable state. The bit is minutes. The settable values range from 1 to 1440 minutes (24 hours).

【Default Configuration】 The default value of minutes is 0 minutes (even if the RADIUS security server is unreachable, the device still sends requests to the RADIUS server).

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 If the device enables the active detection function for a RADIUS security server, the radius-server deadtime time Parameter has no effect on the RADIUS security server; otherwise, the RADIUS security server will be in the unreachable state at the time When the time specified by radius-server deadtime exceeds the time specified by the radius-server deadtime, the device is automatically restored to the reachable state.

【Configuration Example]】1: The following example specifies that the duration of stop sending is 1 minute.

```
AC-FS(config)# radius-server deadtime 1
```

【Verification】Use show radius parameter to view the configuration information of the length of time that the device stops sending request packets to the RADIUS security server in the unreachable state.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.12radius-server host

Specifies the RADIUS security server host.

radius-server host [oob] { ipv4-address | ipv6-address } [auth-port port-number] [acct-port port-number] [test username name [idle-time time] [ignore-auth-port] [ignore-acct-port]] [key [0 | 7] text-string]

Deletes the specified RADIUS security server host.

no radius-server host { ipv4-address | ipv6-address }

【Parameter Description】

Parameter	Description
oob	oob authentication, i.e., the source interface is the mgmt port when sending messages to this server.
ipv4-address	The IPv4 address of the RADIUS secure server host.

ipv6-address	The IPv6 address of the RADIUS secure server host.
auth-port port-number	The UDP port for RADIUS authentication, in the range 0 - 65535, if set to 0, then No authentication for this host.
acct-port port-number	The UDP port for RADIUS accounting, in the range 0 - 65535, if set to 0, then the host does not do accounting.
test username name	Enables active detection Function for this RADIUS security server and specifies the user name to be used for active detection. The user name used for active probing.
idle-time time	Configure the time interval for the device to send test messages to the RADIUS security server in the reachable state. The default value is 60 minutes, and the configurable range is 1-1440 minutes (24 hours).
ignore-auth-port	Disables the detection of the authentication port of the RADIUS security server, which is enabled by default.
ignore-acct-port	Disables detection of the accounting port of the RADIUS secure server, which is enabled by default.
key [0 | 7] text-string	Configure the shared key to be used for this server, or use the global configuration if it is not configured. The configured key can specify the The configured key can specify the encryption type, 0 for no encryption, 7 for simple encryption, and 0 by default.

【Default Configuration】 No RADIUS host specified

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 In order to use RADIUS to implement AAA security service, a RADIUS security server must be defined. You can define one or more RADIUS security servers with the radius-server host command. If the RADIUS security server is not configured in a RADIUS server group, the device uses the global routing table when sending RADIUS packets to the application server; otherwise, the vrf routing table corresponding to the RADIUS server group is used.

【Configuration Example]】 1: The following example defines a RADIUS security server host in an IPv4 environment.

```
AC-FS(config)# radius-server host 192.168.12.1
```

2: The following example defines a RADIUS security server host in an IPv4 environment, enables the active detection function, the detection interval is 60 minutes, and the detection of the accounting UDP port is disabled.

```
AC-FS(config)# radius-server host 192.168.100.1 test username test idle-time 60 ignore-acct-port
```

3: The following example defines a RADIUS security server host in an IPv6 environment.

```
AC-FS(config)# radius-server host 3000::100
```

【Verification】Use show radius server to view the configuration information of the RADIUS security server.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.13radius-server key

Defines the shared password for the network access server (routing device) to communicate with the RADIUS security server.

radius-server key [0 | 7] text-string

Cancel the specified shared password.

no radius-server key

【Parameter Description】

Parameter	Description
text-string	Text of the shared passphrase.
0 | 7	Encryption type of the passphrase, 0 no encryption, 7 simple encryption.

【Default Configuration】 No shared password is specified.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 The shared password is the basis for the correct communication between the device and the RADIUS security server. In order for the device and the RADIUS security server to communicate, the same shared password must be defined on the device and the RADIUS security server.

【Configuration Example]】1: The following example defines the shared password of the RADIUS security server as aaa.

```
AC-FS(config)# radius-server key aaa
```

【Verification】Use show radius server to view the configuration information of the shared password of the RADIUS security server.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.14radius-server retransmit

Configure the number of times that the device resends the packet before it considers that the RADIUS security server has not responded.

radius-server retransmit retries

Restore the default number of retransmissions.

no radius-server retransmit

【Parameter Description】

Parameter	Description
retries	The number of times radius attempts to resend. The value range is 1-100.

【Default Configuration】 The default number of retransmissions is 3.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 AAA uses the next method to authenticate users on the premise that the currently authenticated security server does not respond. The standard for the device to judge that the security server does not respond is that the security server does not respond when the device retransmits the specified number of RADIUS packets, and there is a timeout interval between each retransmission.

【Configuration Example]】1: The following example specifies the number of retransmissions as 4.

```
AC-FS(config)# radius-server retransmit 4
```

【Verification】Use the command show radius parameter to view the configuration information of radius retransmission times.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.15radius-server source-port

Configure the source port for the device to send RADIUS packets.

radius-server source-port port

Restore Defaults.

no radius-server source-port

【Parameter Description】

Parameter	Description
port	The port to set. The range of values that can be set is 1-65535.

【Default Configuration】 Random port.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 The source port of the device sending RADIUS packets is random by default. If you need to specify the source port, use this command to configure it.

【Configuration Example]】1: The following example defines the source port for sending radius packets as 10000.

```
AC-FS(config)# radius-server source-port 10000
```

【Verification】Use show running-config to view the source port configuration information of the device radius packet.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.16radius-server timeout

Configure the time for the device to wait for the security server to reply when resending RADIUS packets.

radius-server timeout seconds

Restore Defaults.

no radius-server timeout

【Parameter Description】

Parameter	Description
seconds	Timeout time (in seconds). The settable values range from 1 to 1000 seconds.

【Default Configuration】 The default is 5 seconds

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Use this command to configure the time for the device to wait for the security server to reply when resending RADIUS packets.

【Configuration Example]】1: The following example defines the timeout as 10 seconds.

```
AC-FS(config)# radius-server timeout 10
```

【Verification】Use show radius parameter to view the configuration information of the time for the device to retransmit RADIUS packets and wait for the response from the security server.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.17radius-server authentication attribute

Configure to carry specified attributes in RADIUS authentication request packets.

radius-server authentication attribute type package

Configure not to carry the specified attribute in the RADIUS authentication request packet.

radius-server authentication attribute type unpackage

Restore the default configuration of whether the attribute specified in the authentication request packet is carried.

no radius-server authentication attribute type package

default radius-server authentication attribute type package

no radius-server authentication attribute type unpackage

default radius-server authentication attribute type unpackage

【Parameter Description】

Parameter	Description
type	RADIUS attribute type. Can be set in the range 1-255.

【Default Configuration】 The RFC mandates that the attributes that must be carried in the authentication request are carried by default, and the attributes that do not need to be carried are stipulated that they are not carried by default. Other attributes are not set by default, which can be carried or not carried.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Use this command to configure whether to send the corresponding attribute in the RADIUS authentication request packet.

The RFC mandates that the attributes that must be carried in the authentication request cannot be changed to not carry, and the attributes that do not need to be carried cannot be changed to carry.

The no and default commands restore the configuration of attributes to their default states.

【Configuration Example]】 1: The following example does not send the NAS-PORT-ID attribute in the RADIUS authentication request packet.

```
AC-FS(config)# radius-server authentication attribute 87 unpackage
```

【Verification】 Capture packets on the RADIUS server and check that the RADIUS request packet should not carry the 87 attribute

3.18radius-server account attribute

Configure to carry specified attributes in RADIUS accounting request packets.

radius-server account attribute type package

Configure not to carry specified attributes in RADIUS accounting request packets.

radius-server account attribute type unpackage

Restore the default configuration that specifies whether the attribute is carried in the accounting request message.

no radius-server account attribute type package

default radius-server account attribute type package

no radius-server account attribute type unpackage

default radius-server account attribute type unpackage

【Parameter Description】

Parameter	Description
type	RADIUS attribute type. Can be set in the range 1-255.

【Default Configuration】 The RFC enforces that the attributes that must be carried in the accounting request are carried by default, and the attributes that do not need to be carried are stipulated that they are not carried by default. Other attributes are not set by default, which can be carried or not carried.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Use this command to configure whether to send the corresponding attribute in the RADIUS accounting request message

The RFC mandates that the attributes that must be carried in the accounting request cannot be changed to not carry, and the attributes that do not need to be carried cannot be changed to carry.

The no and default commands restore the configuration of attributes to their default states.

【Configuration Example】】 1: The following example does not send the NAS-PORT-ID attribute in the RADIUS accounting request message.

```
AC-FS(config)# radius-server account attribute 87 unpackage
```

【Verification】Capture packets on the RADIUS server and check that the RADIUS accounting request message should not carry 87 related

attributes.

3.19radius-server authentication vendor

Configure the RADIUS authentication request packet to carry the private attribute of the relevant manufacturer.

radius-server authentication vendor [cmcc | microsoft | cisco | hw] package

The default configuration is restored, and the private attribute of the relevant manufacturer is not carried in the authentication request packet.

no radius-server authentication vendor vendor_name package

default radius-server authentication vendor vendor_name package

【Parameter Description】

Parameter	Description
cmcc | microsoft | cisco |hw	Manufacturer type, cmcc china mobile, microsoft microsoft, cisco cisco, hw Huawei.

【Default Configuration】 The authentication request message does not carry private attributes of other manufacturers

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Use this command to configure whether the RADIUS authentication request packet carries the private attribute of the specified manufacturer

【Configuration Example]】1: The following example carries the private attribute of cmcc in the RADIUS authentication request packet.

```
AC-FS(config)# radius-server authentication vendor cmcc package
```

【Verification】 When capturing packets on the RADIUS server, you can check that the RADIUS authentication request message should not carry the private attributes required by cmcc

3.20radius-server account vendor

Configure the RADIUS accounting request packet to carry the private attribute of the relevant manufacturer

radius-server account vendor [cmcc | microsoft | cisco | hw] package

The default configuration is restored, and the private attributes of the relevant manufacturer are not carried in the accounting request message

no radius-server account vendor vendor_name package default radius-server account vendor vendor_name package

【Parameter Description】

Parameter	Description
cmcc | microsoft | cisco | hw	Manufacturer type, cmcc china mobile, microsoft microsoft, cisco cisco, hw huawei.

【Default Configuration】 The accounting request message does not carry private attributes of other manufacturers

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Use this command to configure whether the RADIUS accounting request packet carries the private attribute of the specified manufacturer

【Configuration Example】1: The following example carries the private attribute of cmcc in the radius accounting request message.

```
AC-FS(config)# radius-server account vendor cmcc package
```

【Verification】When capturing packets on the RADIUS server, you can check that the RADIUS accounting request message should not carry the accounting attributes required by cmcc.

3.21radius set qos cos

Set the qos value delivered by radius to the interface cos value

radius set qos cos

Restore the qos value delivered by the default radius

no radius set qos cos

【Parameter Description】 -

【Default Configuration】 The default qos configuration is the dscp value.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Set the qos value delivered by radius to the interface cos value.

```
AC-FS(config)# radius set qos cos
```

【Verification】Use show running-config to view the configuration information of qos value.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.22radius support cui

Set radius to support cui property.

radius support cui

Turn off radius support for cui attributes.

no radius support cui

【Parameter Description】 -

【Default Configuration】 The cui attribute is not supported by default.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Use this command to configure whether radius supports cui attribute according to your needs.

【Configuration Example】1: Configure radius to support cui attribute.

```
AC-FS(config)# radius support cui
```

【Verification】Use show running-config to view the support of radius support cui attribute

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.23 server auth-port acct-port

Add a server to the AAA server group, delete it in the form of no.

server { ipv4-addr | ipv6-addr} [auth-port port1] [acct-port port2]

no server { ipv4-addr | ipv6-addr} [auth-port port1] [acct-port port2]

【Parameter Description】

Parameter	Description
ip-addr	Server ip address.
Ipv6-addr	Server ipv6 address.
port1	Server authentication port.
port2	Server bookkeeping port.

【Default Configuration】 Serverless configuration

【Command Mode】Server group configuration mode.

【Default Level】 14

【Usage Guide】 Add a server to the specified server, and use the default value when the port is not specified.

【Configuration Example]】 1: The following example adds server 192.168.4.12 to server group ss and sets its accounting port as 5 and authentication port as 6.

```
AC-FS(config)# aaa group server radius ss
AC-FS(config-gs-radius)# server 192.168.4.12 acct-port 5 auth-port 6
AC-FS(config-gs-radius)# end
AC-FS# show aaa group
Type       Reference  Name
---------- ---------- ----------
radius   1   radius   tacacs+            1
tacacs+
radius     1          ss
```

【Verification】 Use the show radius group command to view the server information of the RADIUS server group.

【Prompt Information】 -

【Related commands】

Commands	Description
aaa group server	Configuring aaa server groups.
show aaa group	Show aaa server groups.

【Common Mistake】 -

【Platform Description】 -

3.24 show radius acct statistics

Displays statistics related to RADIUS accounting.

show radius radius acct statistics

【Parameter Description】 -

【Command Mode】 Global mode, privileged mode, interface mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example】 1: Display RADIUS accounting related statistics.

```
AC-FS#show radius acct statistics
Accounting Servers:

Server Index.....1
Server Address..... 192.168.1.1
Server Port.....1813
Msg Round Trip Time.....0 (msec)
First Requests.....1
Retry Requests.....1
Accounting Responses.....0
Malformed Msgs.....0
Bad Authenticator Msgs.....0
Pending Requests.....1
```

【Prompt Information】-

【Platform Description】 -

3.25 show radius auth statistics

Displays statistics related to RADIUS authentication.

show radius auth statistics

【Parameter Description】 -

【Command Mode】 Global mode, privileged mode, interface mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Display RADIUS authentication related statistics.

```
AC-FS#show radius auth statistics
Authentication Servers:

Server Index.....1
Server Address..... 192.168.1.1
Server Port.....1812
Msg Round Trip Time.....0 (msec)
First Requests.....0
Retry Requests.....0
Accept Responses.....0
Reject Responses.....0
Challenge Responses.....0
Malformed Msgs.....0
Bad Authenticator Msgs.....0
Pending Requests.....0
Timeout Requests.....0
Unknowntype Msgs.....0
Other Drops.....0
```

【Prompt Information】-

【Platform Description】 -

3.26 show radius group

Displays the configuration of the RADIUS server group.

show radius group

【Parameter Description】-

【Command Mode】 Global mode, privileged mode, interface mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Display the configuration of the RADIUS server group.

```
AC-FS#show radius group
==========Radius group radius==========
Vrf:not-set
Server:192.168.1.1
  Server key:AC-FS
  Authentication port:1812
  Accounting port:1813
  State:Active
```

【Prompt Information】-

【Platform Description】 -

3.27 show radius parameter

Displays the global parameters of the RADIUS server.

show radius parameter

【Parameter Description】-

【Command Mode】 Global mode, privileged mode, interface mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Display the global parameters of the RADIUS server.

```
AC-FS# show radius parameter
Server Timout:   5 Seconds
Server Deadtime: 0 Minutes
Server Retries:  3
Server Dead Critera:
Time:  10 Seconds
Tries:       10
```

【Prompt Information】-

【Platform Description】 -

3.28 show radius server

Displays the RADIUS server configuration.

show radius server

【Parameter Description】 -

【Command Mode】 Global mode, privileged mode, interface mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example】 1: Display the RADIUS server configuration.

```
AC-FS# show radius server
Server IP.....192.168.4.12
Accounting Port: 23
Authen  Port:     77
Test Username:  test
Test Idle Time: 10 Minutes
Test Ports:        Authen
Server State:  Active
    Current duration 765s, previous duration 0s
Dead: total time 0s, count 0
Statistics:
Authen: request 15, timeouts 1
Author: request 0, timeouts 0
Account: request 0, timeouts 0

Server IP: 192.168.4.13
Accounting  Port:   45
Authen  Port:  74
Test Username:  <Not Configured>
Test Idle Time: 60 Minutes
Test Ports:        Authen and Accounting
Server State:  Active
Current duration 765s, previous duration 0s
Dead: total time 0s, count 0
Statistics:
Authen: request 0, timeouts 0
```

```
Author: request 0, timeouts 0
Account: request 20, timeouts 0
```

【Prompt Information】-

【Platform Description】 -

3.29 show radius vendor-specific

Displays the RADIUS private attribute type configuration.

show radius vendor-specific

【Parameter Description】-

【Command Mode】 Global mode, privileged mode, interface mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Display RADIUS private attribute type configuration.

```
AC-FS#show  radius  vendor-specific
id    vendor-specific      type-value
_____ ___________________ __________
1          max-down-rate             1
2  port-priority  2  3         user-ip
3
4     vlan-id              4
5     last-supplicant-vers 5
      ion
6     net-ip               6
7     user-name            7
8          password                  8
9          file-directory            9
10  file-count  10
11    file-name-0          11
12    file-name-1          12
13    file-name-2          13
14    file-name-3          14
15    file-name-4          15
```

```
16    max-up-rate          16
17    current-supplicant-v 17
      ersion
18    flux-max-high32      18
19    flux-max-low32       19
20    proxy-avoid          20
21    dialup-avoid         21
22         ip-privilege             22
23         login-privilege          42
26  ipv6-multicast-addre 79
      ss
27  ipv4-multicast-addre 87
      ss
```

【Prompt Information】 -

【Platform Description】 -

4 802.1x

4.1 clear dot1x user all

Delete all dot1x users on the device.

clear dot1x user all

【Parameter Description】-

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】15

【Usage Guide】 Use this command to delete all dot1x authentication users on the device.

【Configuration Example]】1: Delete all dot1x authentication users.

```
AC-FS#clear dot1x user all
```

【Prompt Information】-

【Platform Description】 -

4.2 clear dot1x user id

Delete the corresponding user based on the session id of the dot1x user.

clear dot1x user id session-id

【Parameter Description】

Parameter	Description
- session-id	-dot1x session id of the authenticated user.

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】15

【Usage Guide】 You can use this command when you need to delete the dot1x authentication user with a specific session id.

【Configuration Example]】 1: Delete the dot1x authentication user whose session id is 12345678.

```
AC-FS#clear dot1x user id 12345678
```

【Prompt Information】-

【Platform Description】 -

4.3 clear dot1x user mac

Delete the corresponding user according to the mac of the dot1x user.

clear dot1x user mac mac-addr

【Parameter Description】

Parameter	Description
- mac-addr	-dot1x MAC address of authenticated user.

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】15

【Usage Guide】 You can use this command when you need to delete the dot1x authentication user of a specific mac address.

【Configuration Example]】1: Delete the dot1x authentication user whose mac address is 0012.3456.789A.

```
AC-FS#clear dot1x user mac 0012.3456.789A
```

【Prompt Information】-

【Platform Description】 -

4.4 clear dot1x user name

Delete the corresponding user based on the username of the dot1x user.

clear dot1x user name name-str

【Parameter Description】

Parameter	Description
- name-str	-dot1x username of the authenticated user.

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】15

【Usage Guide】 You can use this command when you need to delete the dot1x authentication user with a specific username.

【Configuration Example]】1: Delete the dot1x authentication user whose username is dot1x-user.

```
AC-FS#clear dot1x user name dot1x-user
```

【Prompt Information】-

【Platform Description】 -

4.5 clear dot1x user ip

Delete the corresponding user according to the ip address of the dot1x user.

clear dot1x user ip ip-addr

【Parameter Description】

Parameter	Description
ip-addr	ip address of the dot1x authenticated user.

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】15

【Usage Guide】 You can use this command when you need to delete the dot1x authentication user of a specific ip.

【Configuration Example]】1: Delete the dot1x authentication user whose ip is 11.1.1.1.

```
AC-FS#clear dot1x user ip 11.1.1.1
```

【Prompt Information】-

【Platform Description】 -

4.6dot1x accounting

Configure the list of authentication methods.

dot1x accounting list-name

【Parameter Description】

Parameter	Description
list-name	List of bookkeeping methods.

【Default Configuration】-

【Command Mode】Global mode, wlan safe mode

【Default Level】15

【Usage Guide】 If the dot1x accounting method of aaa is not the default, you need to use this command to configure the corresponding accounting method.

The accounting method configured under wlansec is higher than the accounting method configured globally

【Configuration Example】1: Configure the list of authenticated hosts.

```
AC-FS(config)# dot1x accounting dot1x-acct
```

【Prompt Information】-

【Platform Description】 -

4.7dot1x acct-update base-on first-time server

Configure and select the accounting update cycle delivered by the server during the first authentication.

dot1x acct-update base-on first-time server

Disable the accounting update cycle delivered by the server during the first authentication.

no dot1x acct-update base-on first-time server

【Parameter Description】

Parameter	Description
-	Default off.

【Default Configuration】Close

【Command Mode】 Global mode

【Default Level】15

【 Usage Guide 】 Some servers will not issue the accounting update cycle when the user is re-authenticated, but require that the accounting update message must be sent according to the accounting update cycle issued by the user when the user is authenticated for the first time. You can configure this command.

【Configuration Example]】 1: Configure the accounting update cycle delivered by the server during the first authentication.

```
AC-FS(config)# dot1x acct-update base-on first-time server
```

【Prompt Information】-

【Platform Description】 -

4.8dot1x auth-fail max-attempt

Configure the number of authentication failure attempts.

dot1x auth-fail max-attempt value

Restore the number of failed authentication attempts.

no dot1x auth-fail vlan

【Parameter Description】

Parameter	Description
value	Number of failed authentication attempts.

【Default Configuration】 The default is 3 times

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 This command can be configured to adjust the authentication failure times of users entering the FAIL VLAN.

【Configuration Example]】1: Configure the number of authentication attempts to 2.

```
AC-FS(config)# dot1x auth-fail max-attempt 2
```

【Prompt Information】-

【Platform Description】 -

4.9dot1x auth-mode

Configure the authentication mode.

dot1x auth-mode { eap | chap | pap }

【Parameter Description】

Parameter	Description
-	default eap.

【Default Configuration】eap mode

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 The choice of authentication mode depends on the support of the supplicant and the authentication server.

【Configuration Example]】 1: Configure the chap authentication mode.

```
AC-FS(config)# dot1x auth-mode eap
```

【Prompt Information】-

【Platform Description】 -

4.10dot1x auth-address-table address

Configure the list of authenticated hosts.

dot1x auth-address-table address mac-addr interface interface

【Parameter Description】

Parameter	Description
mac-addr	The mac address of the authenticated access terminal.
interface	The port where the access terminal is located.

【Default Configuration】-

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 Only the terminal with the specified mac address can perform 802.1x authentication by limiting the specified port.

【Configuration Example】1: Configure the list of authenticated hosts.

```
AC-FS(config)# dot1x auth-address-table 00d0.f800.0cb2 interface fastethernet 0/1
```

【Prompt Information】-

【Platform Description】 -

4.11dot1x authentication

Configure the list of authentication methods.

dot1x authentication list-name

【Parameter Description】

Parameter	Description
list-name	List of authentication methods.

【Default Configuration】-

【Command Mode】Global mode, wlan safe mode

【Default Level】15

【 Usage Guide 】 If the dot1x authentication method of aaa is not the default, you need to use this command to configure the corresponding authentication method.

The authentication method configured under wlansec is higher than the accounting method configured globally

【Configuration Example】1: Configure the list of authenticated hosts.

```
AC-FS(config)# dot1x authentication dot1x-authen
```

【Prompt Information】-

【Platform Description】 -

4.12dot1x auto-req

Configure the device to actively initiate 802.1x authentication.

dot1x auto-req

Disable active authentication.

no dot1x auto-req

【Parameter Description】 -

【Default Configuration】 N18K device is disabled by default, others are enabled by default

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】This function must be enabled when deploying the MAB environment, and the terminal can choose to enable this function using the authentication client that comes with the operating system.

【Configuration Example]】1: Configure active authentication.

```
AC-FS(config)# dot1x auto-req
```

【Prompt Information】-

【Platform Description】 -

4.13 dot1x auto-req packet-num

Configure the number of authentication request packets initiated by the device.

dot1x auto-req packet-num num

【Parameter Description】

Parameter	Description
num	The number of messages sent for active authentication, the default value is 0, which means always send, the configuration range 0-1000000.

【Default Configuration】 0

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】-

【Configuration Example]】1: Configure the number of active authentication packet requests.

```
AC-FS(config)# dot1x auto-req packet-num 100
```

【Prompt Information】-

【Platform Description】 -

4.14 dot1x auto-req req-interval

Configure the interval for the device to actively send authentication request packets.

dot1x auto-req req-interval time

【Parameter Description】

Parameter	Description
time	The interval between messages sent for active authentication, the default value is 30 seconds, the configuration range is 10-363600.

【Default Configuration】 0

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】-

【Configuration Example]】 1: Configure the request interval for active authentication packets.

```
AC-FS(config)# dot1x auto-req req-interval 50
```

【Prompt Information】-

【Platform Description】 -

4.15dot1x auto-req user-detect

Configure active authentication to check whether a user is authenticating.

dot1x auto-req user-detect

Disable active authentication to check whether a user is authenticating.

no dot1x auto-req user-detect

【Parameter Description】 -

【Default Configuration】 Open by default

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】It is recommended to enable this function when placing an order on the port, which can reduce the authentication pressure on the server.

【Configuration Example]】1: Configure active authentication to check whether a user is authenticating.

```
AC-FS(config)# dot1x auto-req user-detect
```

【Prompt Information】-

【Platform Description】 -

4.16dot1x client-probe enable

Configure FS client online detection.

dot1x client-probe enable

Disable FS client online detection.

no dot1x client-probe enable

【Parameter Description】

Parameter	Description
	Default off.

【Default Configuration】 Default off

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】It is recommended to enable this function when using FS supplicant.

【Configuration Example]】1: Configure FS client online detection.

```
AC-FS(config)# dot1x client-probe enable
```

【Prompt Information】-

【Platform Description】 -

4.17dot1x critical

Configure server fail-pass authentication.

dot1x critical

Disable server fail-pass authentication.

no dot1x critical

【Parameter Description】 -

【Default Configuration】 Default off

【Command Mode】 Interface mode, vxlan mode

【Default Level】15

【Usage Guide】RADIUS needs to configure both the account for detecting the reachability of the server and the criterion for judging the unreachable server.

【Configuration Example]】1: Configure server fail-pass authentication.

```
AC-FS(config-if-GigabitEthernet 0/5)#dot1x critical
```

【Prompt Information】-

【Platform Description】 -

4.18 dot1x critical recovery action reinitialize

Configure server fail-pass authentication recovery processing.

dot1x critical recovery action reinitialize

Disable server fail-pass authentication recovery processing.

no dot1x critical recovery action reinitialize

【Parameter Description】 -

【Default Configuration】 Default off

【Command Mode】 Interface mode, vxlan mode

【Default Level】15

【Usage Guide】 When the RADIUS server is reachable again, it is necessary to re-verify whether the authorized user has a legal identity during the server unreachable period. You can use this command.

【Configuration Example]】1: Configure server fail-through authentication recovery processing.

```
AC-FS(config-if-GigabitEthernet 0/5)#dot1x critical recovery action reinitialize
```

【Prompt Information】-

【Platform Description】 -

4.19dot1x critical vlan

Configure the server fail-pass authentication jump VLAN.

dot1x critical vlan vlan-id

Disable server fail-pass authentication jump VLAN.

no dot1x critical vlan

【Parameter Description】

Parameter	Description
vlan-id	VLAN ID of the server failed bypass authentication hop.

【Default Configuration】 Default off

【Command Mode】 Interface mode

【Default Level】15

【Usage Guide】 You can configure this command when you need to provide temporary access to network resources for authenticated users when the server fails.

【Configuration Example]】1: Configure the server fail-pass authentication jump VLAN.

```
AC-FS(config-if-GigabitEthernet 0/5)#dot1x critical vlan 10
```

【Prompt Information】-

【Platform Description】 -

4.20dot1x dbg-filter

Print debug information for a specific mac address.

dot1x dbg-filter H.H.H

Clear debug filter information.

no dot1x dbg-filter H.H.H

【Parameter Description】

Parameter	Description
H.H.H	The Mac address of the user who needs to output debug information.

【Default Configuration】 The debugging information of all authenticated users is printed.

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 When there are a large number of users in the network and you need to locate the fault in the current network, you can use this command to print debugging information to individual users to avoid the device from printing too much debugging information.

【Configuration Example]】1: Configure a specific mac address to print debugging information.

```
AC-FS(config)# dot1x dbg-filter 00d0.f800.0001
```

【Prompt Information】-

【Platform Description】 -

4.21dot1x default-user-limit

Configure the limit on the number of authenticated users on an interface.

dot1x default-user-limit num

Restore Defaults.

no dot1x default-user-limit

【Parameter Description】

Parameter	Description
num	Limit the number of authenticated users under an interface. Parameter range 1 to 1000000. The default is 1,000,000.

【Default Configuration】 1000000

【Command Mode】 Interface mode

【Default Level】15

【Usage Guide】 If you want to limit the number of authenticated users under a port, you can use this command to limit. The default value represents the maximum number of users that can be recorded in 4 bytes.

【Configuration Example]】1: Configure the number of authenticated users under the interface.

```
AC-FS(config-if)# dot1x default-user-limit 10
```

【Prompt Information】-

【Platform Description】 -

4.22dot1x default

Restore the default configuration of dot1x.

dot1x default

【Parameter Description】 -

【Default Configuration】 -

【Command Mode】 Global mode

【Default Level】 15

【Usage Guide】 After configuring a large number of dot1x commands, in order to quickly reconfigure, you can use this command from

【Configuration Example]】 1: Restore dot1x mo, default configuration.

```
AC-FS(config)# dot1x default
```

【Prompt Information】-

【Platform Description】 -

4.23dot1x encryption only

Configure 802.1x to be shared with WEB authentication.

dot1x encryption only

Disable 802.1x shared with WEB authentication.

no dot1x encryption only

【Parameter Description】-

【Default Configuration】 By default, 802.1x and WEB authentication are shared and disabled.

【Command Mode】 wlan safe mode

【Default Level】15

【 Usage Guide 】 When 802.1x and WEB authentication are used together, 802.1x users can use this command only for encryption function.

【Configuration Example]】 1: Configure the sharing of 802.1x and WEB authentication.

```
AC-FS(config-wlansec)#dot1x encryption only
```

【Prompt Information】-

【Platform Description】 Wireless platform support.

4.24dot1x guest-vlan

Configure the wireless guest vlan.

dot1x guest-vlan [vlan]

Turn off the wireless guest vlan.

no dot1x guest-vlan

【Parameter Description】

Parameter	Description
vlan	Configured guest vlan.

【Default Configuration】 By default, no wireless guest vlan is configured.

【Command Mode】 wlan safe mode

【Default Level】 14

【Usage Guide】 In wireless scenarios, you need to configure guest-vlan when supporting vlan jump.

【Configuration Example】1: Configure wireless guest-vlan.

```
AC-FS(config-wlansec)#dot1x guest-vlan 10
```

【Prompt Information】 -

【Platform Description】 Wireless platform support.

4.25dot1x event server-invalid action bypass-wlan

Configure the RADIUS server escape function.

dot1x event server-invalid action bypass-wlan wlan-id

Disable the RADIUS server escape function.

no dot1x event server-invalid action bypass-wlan

【Parameter Description】

Parameter	Description
wlan-id	wlan id of the escape.

【Default Configuration】 The default RADIUS server escape is disabled

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 When the RADIUS is unreachable, you can use this command to switch to the preset wlan.

【Configuration Example】1: Configure the RADIUS server escape function.

```
AC-FS(config)#dot1x event server-invalid action bypass-wlan 10
```

【Prompt Information】-

【Platform Description】 Wireless platform support.

4.26dot1x get-static-ip enable

Configure to obtain a static IP address.

dot1x get-static-ip enable

Turn off Obtain static IP address.

no dot1x get-static-ip enable

【Parameter Description】 -

【Default Configuration】 Close.

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 The wireless terminal uses a static IP address. This function can be enabled when the static IP address needs to be uploaded to the server. Note that the IP address is uploaded to the server through the accounting message. No terminal identification information.

【Configuration Example]】 1: Enable the configuration to obtain a static IP address.

```
AC-FS(config)# dot1x get-static-ip enable
```

【Prompt Information】-

【Platform Description】 -

4.27dot1x logging rate-limit

Configure the syslog rate for online and offline printing of authenticated users.

dot1x logging rate-limit value

Turn off the syslog printed by the authenticated user online and offline.

no dot1x logging

【Parameter Description】

Parameter	Description
value	The default is 5 syslogs/s, and 0 is no speed limit for printing syslogs of authenticated users going up and down.

【Default Configuration】 The default is 5 pieces/s

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 You can use the default rate. If there are a large number of authenticated users going online and offline frequently, you

need to lower the rate to avoid high CPU utilization.

【Configuration Example]】 1: Configure the rate of syslog printing for authenticated users online and offline to 20 entries/s.

```
AC-FS(config)# dot1x logging rate-limit 20
```

【Prompt Information】-

【Platform Description】 Wireless platform support.

4.28dot1x mab-username upper

Configure the MAB authentication username to use uppercase letters.

dot1x mab-username upper

【Parameter Description】 -

【Default Configuration】Close

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 The letters in the MAB authentication username are lowercase letters by default. After this command is configured, the new MAB authentication user name will use uppercase letters to meet the server requirements that require the MAB authentication user name to be uppercase.

【Configuration Example]】1: Configure the mab authentication user name to use uppercase letters.

```
AC-FS(config)# dot1x mab-username upper
```

【Prompt Information】-

【Platform Description】 -

4.29dot1x mab-username format

Configure the mab authentication username format.

dot1x mab-username format [with-dot | with-colon | with-hyphen]

Disable username format configuration

no dot1x mab-username format

【Parameter Description】 -

【Default Configuration】Close

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 Mab authentication requires a user name format of xx-xx-xx-xx-xx-xx, configuration with-hyphen Mab authentication requires a user name format of xxxx.xxxx.xxxx, configure with-dot.

Mab authentication requires a username format of xx:xx:xx:xx:xx:xx, configure with-colon

【Configuration Example]】 1: Configure the mab authentication user name format.

```
AC-FS(config)# dot1x mab-username format with-hyphen
```

【Prompt Information】-

【Platform Description】 -

4.30dot1x mac-auth-bypass

Configure single MAB authentication.

dot1x mac-auth-bypass

Turn off single MAB authentication.

no dot1x mac-auth-bypass

【Parameter Description】

Parameter	Description
-	Default Close

【Default Configuration】 The default single mab function is closed

【Command Mode】 Interface mode

【Default Level】15

【Usage Guide】 Use this function when the port is connected to a single dumb terminal.

【Configuration Example]】1: Configure single MAB authentication.

```
AC-FS(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass
```

【Prompt Information】-

【Platform Description】 -

4.31dot1x mac-auth-bypass multi-user

Configure multi-MAB authentication.

dot1x mac-auth-bypass multi-user

Turn off multi-MAB authentication.

no dot1x mac-auth-bypass multi-user

【Parameter Description】

Parameter	Description
	Default Close.

【Default Configuration】 The default multi-MAB function is disabled.

【Command Mode】 Interface mode, vxlan mode

【Default Level】15

【Usage Guide】 Use this function when multiple dumb terminals are connected to the port.

【Configuration Example]】1: Configure multi-MAB authentication.

```
AC-FS(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass multi-user
```

【Prompt Information】-

【Platform Description】 -

4.32dot1x mac-auth-bypass timeout-activity

Configure the MAB authentication timeout period.

dot1x mac-auth-bypass timeout-activity time

【Parameter Description】

Parameter	Description
time	MAB user can be online time in seconds, default 0, means can be online all the time. Configuration range Range 1-65535.

【Default Configuration】 0 seconds.

【Command Mode】 Interface mode, vxlan mode

【Default Level】15

【Usage Guide】 This parameter can be configured to limit the time that the dumb terminal can access the network.

【Configuration Example]】 1: Configure the MAB authentication timeout period.

```
AC-FS(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass timeout-activity 3600
```

【Prompt Information】-

【Platform Description】 -

4.33dot1x mac-auth-bypass violation

Configure MAB violations.

dot1x mac-auth-bypass violation

Turn off MAB violations

no dot1x mac-auth-bypass violation

【Parameter Description】 -

【Default Configuration】 Default off

【Command Mode】 Interface mode

【Default Level】15

【Usage Guide】This function can be configured when one port is limited to one dumb terminal, which is only applicable to a single MAB environment.

【Configuration Example】1: Configure MAB violation.

```
AC-FS(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass violation
```

【Prompt Information】-

【Platform Description】 -

4.34dot1x mac-auth-bypass vlan

Configure MAB VLANs.

dot1x mac-auth-bypass vlan vlan-list

Disable MAB VLAN.

no dot1x mac-auth-bypass vlan vlan-list

【Parameter Description】

Parameter	Description
vlan-list	List of VLANs allowed for MAB authentication.

【Default Configuration】 Default off

【Command Mode】 Interface mode

【Default Level】15

【Usage Guide】 This command can be configured when only users in some VLANs on the interface are allowed to perform MAB authentication.

【Configuration Example】1: Configure MABVLAN.

```
AC-FS(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass vlan 5, 8-20
```

【Prompt Information】-

【Platform Description】 -

4.35dot1x max-req

Configure the number of retransmissions of request/challenge packets.

dot1x max-req num

【Parameter Description】

Parameter	Description
num	request/challenge message retransmission count, default 3, configured range 1-10.

【Default Configuration】 3

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 Just use the default value.

【Configuration Example]】 1: Configure the retransmission times of request/challenge packets.

```
AC-FS(config)# dot1x max-req 2
```

【Prompt Information】-

【Platform Description】 -

4.36dot1x multi-account enable

The configuration supports one mac using multiple account authentication.

dot1x multi-account enable

Turn off support for one mac to use multiple account authentication.

no dot1x multi-account enable

【Parameter Description】 -

【Default Configuration】 Default off

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 This command needs to be configured if the terminal will switch user names during authentication or re-authentication. Typically, such applications exist in Windows' domain authentication.

【Configuration Example]】 1: The configuration supports one mac to use multiple account authentication.

```
AC-FS(config)# dot1x multi-account enable
```

【Prompt Information】-

【Platform Description】 -

4.37dot1x multi-mab quiet-period

Configure the silent time after multi-MAB authentication failure.

dot1x multi-mab quiet-period time

【Parameter Description】

Parameter	Description
time	Silent time after multiple MAB authentication failures, in seconds, default 0, means no silence. Configuration Range 0-65535, configured to 0 for no silence.

【Default Configuration】 0 seconds

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 Just use the default value.

【Configuration Example]】1: Configure the silent time after multi-MAB authentication fails.

```
AC-FS(config)# dot1x multi-mab quiet-period 2
```

【Prompt Information】-

【Platform Description】 -

4.38dot1x mab-username format

Configure the mab authentication username format.

dot1x mab-username format [with-dot | with-colon | with-hyphen]

Disable username format configuration.

no dot1x mab-username format

【Parameter Description】 -

【Default Configuration】 Close

【Command Mode】Global mode

【Default Level】 15

【Usage Guide】 Mab authentication requires a user name format of xx-xx-xx-xx-xx-xx, configuration with-hyphen

Mab authentication requires a user name format of xxxx.xxxx.xxxx, configure with-dot

Mab authentication requires a username format of xx:xx:xx:xx:xx:xx, configure with-colon

【Configuration Example]】1: Configure the mab authentication user name format.

```
AC-FS(config)# dot1x mab-username format with-hyphen
```

【Prompt Information】-

【Platform Description】 -

4.39dot1x offline-detect

Configure the traffic detection function.

dot1x offline-detect {[interval val] | [flow num]}

Turn off traffic detection

no dot1x offline-detect {[interval val] | [flow num]}

【Parameter Description】

Parameter	Description
val	Time interval for flow detection, default 8 hours.
num	Flow rate threshold, default 0KB.

【Default Configuration】 It is enabled by default on the AC, and disabled by default on the AP.

【Command Mode】 wlan safe mode

【Default Level】 15

【Usage Guide】 Optional configuration.

This command can be configured to prevent the STA from going offline but the device has not fully detected it and continues to charge the user.

The user traffic detection function configured in wlan security mode takes precedence over the globally configured authentication user traffic detection function.

【Configuration Example】1: Configure the multi-traffic detection function.

```
AC-FS(config)# dot1x offline-detect interval 5 flow 20
```

【Prompt Information】-

【Platform Description】 Wireless platform available.

4.40dot1x port-control auto

Configure 802.1x authentication on the port.

dot1x port-control auto

Turn off 802.1x authentication on the port

no dot1x port-control auto

【Parameter Description】 -

【Default Configuration】 Default off

【Command Mode】 Interface mode

【Default Level】15

【Usage Guide】 This command must be configured when deploying 802.1x.

【Configuration Example]】 1: Configure 802.1x authentication on the port.

```
AC-FS(config-if-GigabitEthernet 0/0)# dot1x port-control auto
```

【Prompt Information】-

【Platform Description】 -

4.41dot1x port-control-mode

Configure the port controlled mode.

dot1x port-control-mode { mac-based | port-based | port-based single-host}

The default port controlled mode is mac-based controlled

no dot1x port-control-mode

【Parameter Description】-

【Default Configuration】 The default is controlled based on mac.

【Command Mode】 Interface mode

【Default Level】15

【Usage Guide】Configure MAC-based controlled mode in the scenario that requires every user on the controlled port to pass the authentication to communicate;

After allowing one authenticated user to pass through the controlled port, other users can communicate. You can configure the port-based controlled mode.

In the port-based controlled mode, only the authenticated user can be configured as a dynamic user. You can configure this command.

【Configuration Example】1: Configure the port to be controlled based on the port.

```
AC-FS(config-if-GigabitEthernet 0/0)# dot1x port-control-mode port-based
```

【Prompt Information】-

【Platform Description】 -

4.42dot1x probe-timer interval

Configure the FS client detection cycle.

dot1x probe-timer interval time

【Parameter Description】

Parameter	Description
time	Client detection period, in seconds, default 20. configuration range 1-65535.

【Default Configuration】 20 seconds.

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 Just use the default value.

【Configuration Example]】1: Configure the FS client detection cycle.

```
AC-FS(config)# dot1x probe-timer interval 30
```

【Prompt Information】-

【Platform Description】 -

4.43 dot1x probe-timer alive

Configure the detection duration of FS client.

dot1x probe-timer alive time

【Parameter Description】

Parameter	Description
time	The client detection duration, in seconds, is 250 by default. Configuration range 1-65535.

【Default Configuration】 250

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】After the terminal is authenticated and goes online, if the device does not receive any detection packet response from the terminal within the detection period, the terminal is considered offline. It is recommended to use the default value.

【Configuration Example]】1: Configure the detection duration of Ruijie client.

```
AC-FS(config)# dot1x probe-timer alive 120
```

【Prompt Information】-

【Platform Description】 -

4.44dot1x private-supplicant-only

Configure the function of filtering non-FS clients.

dot1x private-supplicant-only

Disable the function of filtering non-FS clients

no dot1x private-supplicant-only

【Parameter Description】-

【Default Configuration】 Default off

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 If the deployment environment requires the use of FS supplicant software certification, you can configure this function.

【Configuration Example]】1: Configure the function of filtering non-FS clients.

```
AC-FS(config)# dot1x private-supplicant-only
```

【Prompt Information】-

【Platform Description】 -

4.45dot1x pseudo source-mac

Configure the virtual mac as the source mac address of 802.1x packets sent by the device.

dot1x pseudo source-mac

Disable the use of virtual mac as the source mac address of 802.1x packets sent by the device

no dot1x pseudo source-mac

【Parameter Description】-

【Default Configuration】 Open by default.

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 By default, the device uses the mac address of the device as the source mac address of eap packets during 802.1x authentication. Some versions of FS supplicant will judge whether the access device is a FS device according to the source mac address of the eap packet, and implement some private features. When doing 802.1x authentication with these supplicants, if you want to use the relevant private features, You can enable the virtual source mac address function.

【Configuration Example]】1: Configure to use virtual mac as the source mac address of 802.1x packets sent by the device.

```
AC-FS(config)# dot1x pseudo source-mac
```

【Prompt Information】-

【Platform Description】 -

4.46 dot1x redirect

Configure the second-generation su upgrade function.

dot1x redirect

Disable the second-generation su upgrade function

no dot1x redirect

【Parameter Description】

Parameter	Description
	Default Close.

【Default Configuration】 Default off

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 To download the supplicant software by redirecting to the specified resource website through the browser, you need to configure the redirection parameters. For details, refer to the Description in the web authentication configuration manual.

【Configuration Example]】1: Configure the second-generation su upgrade function.

```
AC-FS(config)# dot1x redirect
```

【Prompt Information】-

【Platform Description】 -

4.47dot1x reauth-max

Configure the number of retransmissions of request/id packets.

dot1x reauth-max num

【Parameter Description】

Parameter	Description
num	request/id number of message retransmissions, default 3, configured range 1-10.

【Default Configuration】 3

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 Just use the default value.

【Configuration Example]】 1: Configure the number of retransmissions of request/id packets.

```
AC-FS(config)# dot1x reauth-max 2
```

【Prompt Information】-

【Platform Description】 -

4.48 dot1x re-authentication

Configure the re-authentication function.

dot1x re-authentication

Disable re-authentication.

no dot1x re-authentication

【Parameter Description】-

【Default Configuration】 Default off

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 The re-authentication function will put pressure on the server. In an environment with a large number of users, it is recommended to disable this function.

【Configuration Example]】1: Configure the re-authentication function.

```
AC-FS(config)# dot1x re-authentication
```

【Prompt Information】-

【Platform Description】 -

4.49dot1x stationarity enable

Configure to disable dynamic user migration.

dot1x stationarity enable

Turn off prohibit dynamic user migration

no dot1x stationarity enable

【Parameter Description】-

【Default Configuration】 The default dynamic user can be migrated.

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 Do not allow dynamic users based on port-controlled mode to migrate to other ports. You can configure this command.

【Configuration Example]】 1: The configuration prohibits dynamic user migration.

```
AC-FS(config)# dot1x stationarity enable
```

【Prompt Information】-

【Platform Description】 -

4.50dot1x timeout re-authperiod

Configure the re-authentication interval.

dot1x timeout re-authperiod time

【Parameter Description】

Parameter	Description
time	Re-authentication interval, in seconds, default 3600, configuration range 1-65535

【Default Configuration】 3600 seconds.

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 Just use the default value.

【Configuration Example]】 1: Configure the re-authentication interval.

```
AC-FS(config)# dot1x timeout re-authperiod 2400
```

【Prompt Information】-

【Platform Description】 -

4.51dot1x timeout quiet-period

Configure the silent time after authentication failure.

dot1x timeout quiet-period time

【Parameter Description】

Parameter	Description

time	Quiet time after authentication failure, in seconds, default 10, configured range 1-65535535.

【Default Configuration】 10

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 Just use the default value.

【Configuration Example]】1: Configure the silent time after authentication failure.

```
AC-FS(config)# dot1x timeout quiet-period 60
```

【Prompt Information】-

【Platform Description】 -

4.52dot1x timeout supp-timeout

Configure the request/challenge packet retransmission interval.

dot1x timeout supp-timeout time

【Parameter Description】

Parameter	Description
time	retransmission interval, unit: s, default: 3, configuration range: 1-65535.

【Default Configuration】 3 seconds

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 Just use the default value.

【Configuration Example]】1: Configure the request/challenge packet retransmission interval.

```
AC-FS(config)# dot1x timeout supp-timeout 10
```

【Prompt Information】-

【Platform Description】 -

4.53dot1x timeout server-timeout

Configure the server timeout period.

dot1x timeout server-timeout time

【Parameter Description】

Parameter	Description
time	Server timeout, unit: seconds, default: 5, configuration range: 1-65535.

【Default Configuration】5 seconds

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 It must be ensured that the 802.1x server timeout value is greater than the radius timeout value. By default, the 802.1x timeout value is less than the radius timeout value. Therefore, the actual use is mainly to reduce the radius server timeout value. For details, please refer to the configuration manual of radius.

【Configuration Example】1: Configure the server timeout time.

```
AC-FS(config)# dot1x timeout server-timeout 10
```

【Prompt Information】-

【Platform Description】 -

4.54dot1x timeout tx-period

Configure the request/id packet retransmission interval.

dot1x timeout tx-period time

【Parameter Description】

Parameter	Description
time	request/id message retransmission interval, in seconds, default 3, configured range 1-6.

【Default Configuration】 3 seconds

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 Just use the default value.

【Configuration Example】1: Configure the server timeout time.

```
AC-FS(config)# dot1x timeout tx-period 5
```

【Prompt Information】-

【Platform Description】 -

4.55dot1x user-trap enable

Configure the function of sending traps when authenticated users go online and offline.

dot1x user-trap enable

Disable the function of sending traps when authenticated users go online and offline.

no dot1x user-trap enable

【Parameter Description】-

【Default Configuration】 Default off

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 You can configure this command when you need to send trap messages of user online and offline to the SNMP server.

【Configuration Example]】1: Enable the function of sending traps when authenticated users go online and offline.

```
AC-FS(config)# dot1x user-trap enable
```

【Prompt Information】-

【Platform Description】 Supported on wireless devices.

4.56dot1x valid-ip-acct enable

Configure the function of initiating accounting after a user obtains an IP.

dot1x valid-ip-acct enable

Disable the function of initiating billing after a user obtains an IP.

no dot1x valid-ip-acct enable

【Parameter Description】

Parameter	Description
-	Default Close.

【Default Configuration】 Default off

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 This function can be configured if the server requires that the authentication user must carry the IP address in the accounting message.

【Configuration Example]】 1: The user initiates accounting after obtaining the IP.

```
AC-FS(config)# dot1x valid-ip-acct enable
```

【Prompt Information】-

【Platform Description】 -

4.57dot1x valid-ip-acct timeout

After the user is authenticated, it is allowed to wait for the user to obtain the IP.

dot1x valid-ip-acct timeout time

Restore Defaults.

no dot1x valid-ip-acct timeout

【Parameter Description】

Parameter	Description
- time	Timeout time, default is 5 minutes.

【Default Configuration】 The default is 5 minutes.

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 When the user can start accounting after obtaining the IP, in order to prevent the client from not obtaining the IP for a long time and not initiating accounting, you can configure the timeout period as needed.

【Configuration Example]】1: After the user is authenticated, the time allowed to wait for the user to obtain an IP.

```
AC-FS(config)# dot1x valid-ip-acct timeout 10
```

【Prompt Information】-

【Platform Description】 -

4.58dot1x-mab

Configure the wireless on-mab function.

dot1x-mab

Restore Defaults.

no dot1x-mab

【Parameter Description】 -

【Default Configuration】 Disable mab function.

【Command Mode】 wlan safe mode

【Default Level】15

【Usage Guide】 Optional configuration.

The client needs to use its mac under WLAN. Configure this command when security authentication is required.

【Configuration Example】1: Enable the wireless mab function.

```
AC-FS(config-wlansec)# dot1x-mab
```

【Prompt Information】-

【Platform Description】 Only supported by wireless platforms.

4.59show dot1x

View 802.1x protocol parameters.

show dot1x

【Parameter Description】

【Default Configuration】-

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】15

【Usage Guide】 Use this command to view the current 802.1x protocol parameters, number of users and other information.

【Configuration Example]】1: View the 802.1x protocol parameters.

```
AC-FS#show dot1x

802.1X basic information:
  802.1X Status.....enable
  Authentication Mode.....eap
  Authorization mode.....disable
  Total User Number.....0 (exclude dynamic user)
  Authenticated User Number.....0 (exclude dynamic user)
  Dynamic User Number.....0
  Re-authentication..... disable
  Re-authentication Period.....3600 seconds
  Re-authentication max.....3 times
  Quiet Period.....10 seconds
  Tx Period.....30 seconds
  Supplicant Timeout.....3 seconds
  Server Timeout.....5 seconds
  Maximum Request.....3 times
  Client Online Probe.....disable
  Eapol Tag.....enable
  802.1x redirect.....disable
  Private supplicant only.....disable
```

Field Description:

Field	Description
802.1X Status	Is 802.1x function configured
Authentication Mode	Authentication mode
Total User Number	The total number of currently authenticated users, including those being authenticated and those who have been authenticated
Authed User Number	Number of currently authenticated users
Dynamic User Number	The number of dynamic users in port mode
Re-authentication	Reconstruct authentication switch state
Re-authentication Period	Period The re-authentication period
Re-authentication max	Max Maximum number of re-authentications
Qu et Period	The silent period after authentication failure
Tx Period	Message retransmission interval
Supplicant Timeout	Request/challenge message retransmission interval
Server Timeout	Server timeout

Maximum Request	Maximum number of requests
Client Online Probe	Client Online Probe Switch
Eapol Tag	Eapol message with tag switch
802.1x redirect	Second generation su upgrade Function switch
Private supplicant only	Private client Probe switch

【Prompt Information】-

【Platform Description】 -

4.60 show dot1x auth-address-table

View the list of certifiable hosts.

show dot1x auth-address-table [address addr] [interface interface]

【Parameter Description】 -

【Default Configuration】-

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】15

【Usage Guide】 Use the list of certifiable hosts.

【Configuration Example]】1: View the list of authenticated hosts.

```
AC-FS #show dot1x auth-address-table
Interface                Address

Fa0/1                    00d0.f800.0c0e
Fa0/2                    001a.c800.0102

AC-FS #show dot1x auth-address-table interface fastEthernet 0/1 Interface
Address
```

```
Fa0/1                          00d0.f800.0c0e

AC-FS #show dot1x auth-address-table address 00d0.f8.00.0c0e Interface
Address

Fa0/1                          00d0.f800.0c0e
```

Field Description:

Field	Description
Interface	Interface Port
Address	Address The mac address of the authenticated host.

【Prompt Information】-

【Platform Description】 -

4.61 show dot1x auto-req

View active authentication status and Parameter.

show dot1x auto-req

【Parameter Description】 -

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】15

【Usage Guide】 Use this command to view the status and parameters of the 802.1x active authentication function.

【Configuration Example]】 1: View the functional status and parameters of active authentication.

```
AC-FS# show dot1x auto-req
Auto-Req: Enabled
User-Detect : Enabled
```

```
Packet-Num  : 0
Req-Interval: 30 Seconds
```

Field Description:

Field	Description
Auto-Req	Active authentication of Function status.
User-Detect	User detection Function status.
Req-Interval	Active authentication message sending interval.

【Prompt Information】-

【Platform Description】 -

4.62 show dot1x max-req

View the number of retransmissions of request/challenge packets.

show dot1x max-req

【Parameter Description】-

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】15

【Usage Guide】 Use this command to view the retransmission times of request/challenge packets.

【Configuration Example]】1: View the number of retransmissions of request/challenge packets

```
AC-FS#show dot1x max-req

Max-Req: 3 Times
```

Field Description:

Field	Description
Max-Req	Request/challenge packet retransmission times.

【Prompt Information】-

【Platform Description】 -

4.63 show dot1x port-control

View controlled port information.

show dot1x port-control [interface interface-type interface-number]

【Parameter Description】

Parameter	Description
interface-type	Port Type.
interface-number	Port Number.

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】 15

【Usage Guide】 Use this command to view the information of the controlled port.

【Configuration Example】 1: View controlled port information.

```
AC-FS#show dot1x port-control
Interface Mode       Dynamic-User Static-User Max-User  Authened MAB
————————— —————————— ———————————— ———————————— ————————— ———————— ————————

Gi0/5     mac-based  0            0           unlimited no       disable
```

Field Description:

Field	Description
Interface	Controlled Port Name
Mode	Port Mode
Dynamic-User	Number of dynamic users on the port
Static-User	Port static user number
Max-User	Port maximum number of users
Authened	The status of whether the port is authenticated or not
MAB	The status of the port configuration MAB authentication

【Prompt Information】 -

【Platform Description】 -

4.64 show dot1x private-supplicant-only

Check the status of the switch to filter non-FS clients.

show dot1x private-supplicant-only

【Parameter Description】-

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】15

【Usage Guide】 Use this command to view the status of the switch for filtering non-FS clients.

【Configuration Example]】 1: View the status of the switch for filtering non-FS clients

```
AC-FS#show dot1x private-supplicant-only

private-supplicant-only: Disabled
```

Field Description:

Field	Description
private-supplicant-only	Filters the status of non-FSclient switches.

【Prompt Information】-

【Platform Description】 -

4.65show dot1x probe-timer

View the Parameter of the client probe.

show dot1x probe-timer

【Parameter Description】 -

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】15

【Usage Guide】 Use this command to view the parameters of the client detection function.

【Configuration Example]】1: View the Parameter of the client detection function

```
AC-FS#show dot1x probe-timer
Hello Interval  : 20
Hello Alive       : 60
```

Field Description:

Field	Description
Hello Interval	Detection cycle
Hello Alive	Detection time

【Prompt Information】-

【Platform Description】 -

4.66 show dot1x re-authentication

Check the status of the reauthentication switch.

show dot1x re-authentication

【Parameter Description】

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】15

【Usage Guide】 Use this command to view the status of the re-authentication switch.

【Configuration Example]】1: View the status of the re-authentication switch

```
AC-FS#show dot1x re-authentication

Reauth-Enabled: Disabled
```

Field Description:

Field	Description
Reauth-Enabled	Re-authentication switch status

【Prompt Information】-

【Platform Description】 -

4.67 show dot1x reauth-max

View the number of retransmissions of request/id packets.

show dot1x reauth-max

【Parameter Description】-

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】15

【Usage Guide】 Use this command to view the retransmission times of request/id packets.

【Configuration Example]】1: View the number of retransmissions of request/id packets

```
AC-FS#show dot1x reauth-max

Reauth-Max: 3 Times
```

Field Description:

Field	Description
Reauth-Max	Request/id message retransmission count.

【Prompt Information】-

【Platform Description】 -

4.68 show dot1x summary

View the authentication user entry information.

show dot1x summary

【Parameter Description】 -

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】15

【 Usage Guide 】 View the information of the authentication user entry. Through this information, you can know what stage the authentication terminal is currently in, such as being authenticated, authenticated, or silent.

【Configuration Example]】 1: View the information of the authentication user entry.

```
AC-FS#show dot1x summary
ID       User       MAC             Interface VLAN Auth-State      Backend-State Port-Status
User-Type Time
```

Field Description:

Field	Description
ID	The IDs obtained from the AAA can be viewed using the show aaa user all command against
User	User name
MAC	The mac address of the authenticated terminal
Interface0	Port of the authentication terminal
VLAN	The vlan id of the authentication terminal
Auth-State	Authentication status machine status
Backend-State	Authentication status machine status
Port-State	Port authentication status
User-Type	Authentication type
Time	Online time

【Prompt Information】-

【Platform Description】 -

4.69show dot1x summary by-ap

View authentication user entry information based on ap.

show dot1x summary by-ap ap-name

【Parameter Description】

Parameter	Description
ap-name	Name of ap.

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】15

【Usage Guide】 View the authentication user entry information according to the ap. Through this information, you can know what stage the authentication terminal is currently in, such as being authenticated, authenticated, or silent.

【Configuration Example]】 1: View the information of the authentication user entry.

```
AC-FS#show dot1x summary by-ap ap1
AP-NAME:ap1
ID User MAC Interface VLAN INNER-VLAN Auth-State
Backend-State Port-Status User-Type Time

1 a03be38... a03b.e38e.0565 wlan 1 1 Authenticated Idle Authed static 0days
0h 0m 4s
```

Field Description:

Field	Description
ID	The IDs obtained from AAA can be viewed against the show aaa user all command.
User	User name
MAC	The mac address of the authenticated terminal
Interface0	Port of the authentication terminal
VLAN	vlan id of the authentication terminal
INNER-VLAN	The inner vlan id where the authentication terminal is located; the Field is supported on the device that supports double-layer tag for authentication users.

Auth-State	Authentication front-end state machine state
Backend-State	Authentication back-end state machine status
Port-State	Port authentication status
User-Type	Authentication type
Time	Online time

【Prompt Information】 The terminal roams from ap1 to ap2, then the authentication information displayed here is still in ap1.

【Platform Description】 -

4.70show dot1x summary by-ap-group

View authentication user entry information based on ap.

show dot1x summary by-ap-group ap-group-name

【Parameter Description】

Parameter	Description
ap-group-name	ap group name

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】15

【Usage Guide】 View the authentication user entry information based on the ap group. Through this information, you can know what stage the authentication terminal is currently in, such as being authenticated, authenticated, or silent.

【Configuration Example]】1: View the information of the authentication user entry.

```
AC-FS#show dot1x summary by-ap-group apgroup1
AP-GROUP-NAME:apgroup1
ID User MAC Interface VLAN INNER-VLAN Auth-State
Backend-State Port-Status User-Type Time

1 a03be38... a03b.e38e.0565 wlan 1 1 Authenticated Idle Authed static 0days
0h 0m 4s
```

Field Description:

Field	Description
ID	The IDs obtained from AAA can be viewed against the show aaa user all command.
User	User name.
MAC	The mac address of the authentication terminal.
Interface0	Authentication terminal port.
VLAN	The vlan id of the authentication terminal.
INNER-VLAN	Authentication terminal is located in the inner vlan id, which supports the Field on the device that supports the double-layer tag of the authenticated user.
Auth-State	Authenticating front-end state machine state.
Backend-State	Authentication back-end state machine state.
Port-State	Port Authentication Status.
User-Type	Authentication Type.
Time	Online Time.

【Prompt Information】 The terminal roams from ap1 to ap2, then the authentication information displayed here is still in ap1.

【Platform Description】 -

4.71show dot1x timeout quiet-period

View the silent time after authentication failure.

show dot1x timeout quiet-period

【Parameter Description】 -

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】15

【Usage Guide】 View the silent time after authentication failure.

【Configuration Example]】1: View the silent time after authentication failure.

```
AC-FS#show dot1x timeout quiet-period

Quiet-Period: 10 Seconds
```

Field Description:

Field	Description
Quiet-Period	Quiet time after authentication failure.

【Prompt Information】-

【Platform Description】 -

4.72 show dot1x timeout re-authperiod

View the reauthentication interval.

show dot1x timeout re-authperiod

【Parameter Description】-

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】15

【Usage Guide】 View the re-authentication interval.

【Configuration Example]】 1: View the re-authentication interval.

```
AC-FS#show dot1x timeout re-authperiod

Reauth-Period: 3600 Seconds
```

Field Description:

Field	Description
Reauth-Period	reauthentication interval.

【Prompt Information】-

【Platform Description】 -

4.73 show dot1x timeout server-timeout

Check the server timeout period.

show dot1x timeout server-timeout

【Parameter Description】 -

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】15

【Usage Guide】 View the server timeout time.

【Configuration Example】1: View the server timeout time.

```
AC-FS#show dot1x timeout server-timeout

Server-Timeout: 5 Seconds
```

Field Description:

Field	Description
Server-Period	Server timeout time

【Prompt Information】-

【Platform Description】 -

4.74 show dot1x timeout supp-timeout

View the request/challenge packet retransmission interval.

show dot1x timeout supp-timeout

【Parameter Description】 -

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】15

【Usage Guide】 View the request/challenge packet retransmission interval.

【Configuration Example]】 1: View the request/challenge packet retransmission interval.

```
AC-FS#show dot1x timeout supp-timeout

Supp-Timeout: 3 Seconds
```

Field Description:

Field	Description
Supp-Timeout	Request/challenge message retransmission interval.

【Prompt Information】-

【Platform Description】 -

4.75 show dot1x timeout tx-period

View the request/id packet retransmission interval.

show dot1x timeout tx-period

【Parameter Description】 -

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】 15

【Usage Guide】 View the request/id packet retransmission interval.

【Configuration Example]】 1: View the request/id packet retransmission interval.

```
AC-FS#show dot1x timeout tx-period

Tx-Period: 30 Seconds
```

Field Description:

Field	Description
Tx-Period	request/id message retransmission interval.

【Prompt Information】-

【Platform Description】 -

4.76 show dot1x user id

View user details based on user id.

show dot1x user id id

【Parameter Description】

Parameter	Description
-id	-The id of the authenticated user.

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】15

【Usage Guide】 Use show dot1x summary to view user profile information, select the user's id, and use this command to further view user information.

【Configuration Example]】1: View the details of the authenticated user

```
AC-FS#show dot1x user id 16777225

User name: ts-user
User id: 16777225
Type: static
Mac address is 0023.aeaa.4286
Vlan id is 2
Access  from  port  Gi0/5
Time online: 0days 0h 0m17s
User ip address is 192.168.3.21
Max user number on this port is 0
Authorization session time is 1000 seconds
Supplicant is private
Start accounting
Permit proxy user
Permit dial user
IP privilege is 0
 user acl-name ts-user_6_0_0 :
```

Field Description:

Field	Description
User name	User name
User id	User id
Type	User type
Mac address	User's mac address
Vlan id	User's vlan id
Access from port	User's port
Time online	User's online time
User ip address	User's IP address
Max user number on this port	Maximum number of users on the port
Authorization session time	The authorization time of the user
Supplicant is private	Whether the user's client is our company su
Start accounting	The user is using bookkeeping
Permit proxy user	Allow this user to proxy
Permit dial user	Allow this user to dial up
IP privilege	The user's IP privilege level
user acl-name	The user's downstream ACL information

【Prompt Information】 -

【Platform Description】 -

4.77 show dot1x user mac

View user details based on user mac.

show dot1x user mac mac-addr

【Parameter Description】

Parameter	Description
-mac-addr	-MAC address of the authenticated user.

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】 15

【Usage Guide】 Use show dot1x summary to view user profile information, select the user's mac, and use this command to further view user information.

【Configuration Example]】 1: View the details of the authenticated user.

```
AC-FS#show dot1x user mac 0023.aeaa.4286

User name: ts-user
User id: 16777225
Type: static
Mac address is 0023.aeaa.4286
Vlan id is 2
Access  from  port  Gi0/5
Time online: 0days 0h 0m17s
User ip address is 192.168.3.21
Max user number on this port is 0
Authorization session time is 1000 seconds
Supplicant is private
Start accounting
Permit proxy user
Permit dial user
IP privilege is 0
 user acl-name ts-user_6_0_0 :
```

Field Description:

Field	Description
User name	User name
User id	User id
Type	User type
Mac address	User's mac address
Vlan id	User's vlan id
Access from port	User's port
Time online	User's online time
User ip address	User's IP address
Max user number on this port	Maximum number of users on the port
Authorization session time	The authorization time of the user
Supplicant is private	Whether the user's client is our company su
Start accounting	The user is using bookkeeping
Permit proxy user	Allow this user to proxy
Permit dial user	Allow this user to dial up

IP privilege	The user's IP privilege level
user acl-name	The user's downstream ACL information

【Prompt Information】-

【Platform Description】 -

4.78 show dot1x user name

View user details based on user mac.

show dot1x user name name

【Parameter Description】

Parameter	Description
-name	-Username string of the authenticated user.

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】15

【Usage Guide】 Use show dot1x summary to view the user profile information, select the user of the user, and use this command to further view the user information.

【Configuration Example]】1: View the details of the authenticated user.

```
AC-FS#show dot1x user name ts-user

User name: ts-user
```

```
User id: 16777225
Type: static
Mac address is 0023.aeaa.4286
Vlan id is 2
Access  from  port  Gi0/5
Time online: 0days 0h 0m17s
User ip address is 192.168.3.21
Max user number on this port is 0
Authorization session time is 1000 seconds
Supplicant is private
Start accounting
Permit proxy user
Permit dial user
IP privilege is 0
 user acl-name ts-user_6_0_0 :
```

Field Description:

Field	Description
User name	User name
User id	User id
Type	User type
Mac address	User's mac address
Vlan id	User's vlan id
Access from port	User's port
Time online	User's online time
User ip address	User's IP address
Max user number on this port	Maximum number of users on the port
Authorization session time	The authorization time of the user
Supplicant is private	Whether the user's client is our company su
Start accounting	The user is using bookkeeping
Permit proxy user	Allow this user to proxy
Permit dial user	Allow this user to dial up
IP privilege	The user's IP privilege level
user acl-name	The user's downstream ACL information

【Prompt Information】-

【Platform Description】 -

5 ARP Check

5.1arp-check

Enable ARP packet inspection.

arp-check

Disable ARP packet inspection.

no arp-check

【Parameter Description】 -

【Default Configuration】 Disable ARP Check function

【Command Mode】 Interface configuration mode, wireless security configuration mode or wireless ap-config all configuration mode

【Default Level】 14

【Usage Guide】 According to the legal user information of the security application module, the corresponding ARP filtering information is generated to realize the filtering of illegal ARP packets in the network. Turning on the ARP Check function in the wireless ap-config all mode is equivalent to turning on the ARP Check function on the wired ports of all APs.

【Configuration Example】The following is an example of enabling ARP Check on port GigabitEthernet 0/1:

```
AC-FS# configure terminal
AC-FS(config)# interface GigabitEthernet 0/1 AC-
FS(config-if-GigabitEthernet 0/1)# arp-check AC-
FS(config-if-GigabitEthernet 0/1)# end AC-FS#
configure terminal
AC-FS(config)# wlansec 1 AC-
FS(config-wlansec)# arp-check
AC-FS(config-wlansec)# end
```

【Verification】1: Use the show interface arp-check list command to view the ARP Check entries that actually take effect on the interface.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

5.2show interface arp-check list

Check the ARP Check entries that actually take effect on the interface.

show { interface [interface-type interface-number] | wlan [wlan-id] } arp-check list

【Parameter Description】

Parameter	Description
interface-type	The type of wired interface.
interface-number	Wired interface number.
wlan-id	Wireless WLAN ID.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Execute this command to view the configuration of the current IP source address binding database.

【Configuration Example】The following is a display example:

```
AC-FS(config)#show interface arp-check list
INTERFACESENDER MAC      SENDER IP  POLICY SOURCE
-----------------------------------------------------------------------------------------------------

GigabitEthernet 0/1                    00D0.F800.0003    192.168.1.3              address-bind
GigabitEthernet  0/1                    00D0.F800.0001      192.168.1.1            port-security
GigabitEthernet  0/4                                                                192.168.1.3
port-security  GigabitEthernet  0/5                          00D0.F800.0003        192.168.1.3
address-bind GigabitEthernet 0/7                    00D0.F800.0006     192.168.1.6          AAA
ip-auth-mode  GigabitEthernet  0/8                00D0.F800.0007       192.168.1.7           GSN
AC-FS(config)#show wlan arp-check list
INTERFACESENDERMAC      SENDERIP  POLICYSOURCE
-----------------------------------------------------------------------------------------------------

WLAN 1                          00D0.F800.0008    192.168.1.8              GSN
```

Field Description:

Field	Description
INTERFACE	Interface Name.
SENDER MAC	Source MAC Address.
SENDER IP	Source IP address.
POLICY SOURCE	Record source.

【Prompt Information】-

【Platform Description】 -

6 Anti-Gateway ARP Spoofing

6.1 anti-arp-spoofing ip

Set up anti-gateway arp spoofing.

anti-arp-spoofing ip ip-address

Remove anti-gateway arp spoofing.

no anti-arp-spoofing ip ip-address

【Parameter Description】

Parameter	Description
ip-address	Gateway IP Address.

【Default Configuration】 This function does not take effect by default.

【Command Mode】 Wireless security configuration mode

【Default Level】 14

【Usage Guide】 1. -

【Configuration Example]】1: Set the anti-gateway arp spoofing function.

```
AC-FS(config)#wlansec 1
AC-FS(config-wlansec)#anti-arp-spoofing ip 192.168.1.1
```

【Verification】show run View the configuration, there are configured commands.

show anti-arp-spoofing Displays anti-gateway arp spoofing information on the interface.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.2show anti-arp-spoofing

Display anti-gateway arp spoofing information on all interfaces.

show anti-arp-spoofing

【Parameter Description】 -

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Display anti-gateway arp spoofing information on all interfaces

【Configuration Example]】 1: Display anti-gateway arp spoofing information on all interfaces.

```
AC-FS#show anti-arp-spoofing
NO    PORT       IP              STATUS
_____ __________ _______________ __________
```

1 Gi0/1 192.168.1.1 active

Field Description:

Field	Description
NO	Serial number.
PORT	Port Information.
IP	Gateway IP address.
STATUS	Table entry effective status.

【Prompt Information】 -

【Platform Description】 -

7 Global IP+MAC binding

7.1 address-bind ipv6-mode

Change IPv6 address binding mode.

address-bind ipv6-mode { compatible | loose | strict }

restore default mode.

no address-bind ipv6-mode

【Parameter Description】

Parameter	Description
compatible	Compatible Mode
loose	Loose Mode
strict	Strict Mode

【Default Configuration】 Strict mode

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】 1: Change the IPv6 address binding mode:

```
AC-FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z. AC-
FS(config)# address-bind ipv6-mode compatible
```

【Verification】Use the show run command to view.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8 DHCP Snooping

8.1 clear ip dhcp snooping binding

To delete all dynamic users in the DHCP Snooping database, this command needs to be executed in privileged mode.

clear ip dhcp snooping binding [ip] [mac] [vlan vlan-id] [interface interface-id | wlan wlan-id]

【Parameter Description】

Parameter	Description
mac	Specifies the MAC address of the user to be deleted.
vlan-id	Specifies the vlan id of the deleted user.
ip	Specifies the IP address of the deleted user.
interface-id	Specifies the interface to which the deleted user belongs.
wlan-id	Specifies the WLAN to which the deleted user belongs.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Execute this command to delete all dynamic users in the DHCP snooping database.

After executing this command, all DHCP users connected to the interface with the IP Source Guard function enabled need to apply for an address again, otherwise they cannot access the network.

【Configuration Example]】 1: The following example deletes all dynamic users in the DHCP snooping database:

```
AC-FS# clear ip dhcp snooping binding
AC-FS# show ip dhcp snooping binding
Total number of bindings: 0
NO.   MACADDRESS          IPADDRESS       LEASE(SEC)   TYPE          VLAN  INTERFACE
_____ _________________ _______________ ____________ _____________ _____ ______________________
```

【Prompt Information】 -

【Platform Description】 -

8.2ip dhcp snooping

Enable the global DHCP Snooping function.

ip dhcp snooping

Disable the global DHCP snooping function.

no ip dhcp snooping

【Parameter Description】 -

【Default Configuration】 This function is disabled by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 After enabling the global DHCP snooping function, you can use the show ip dhcp snooping command to check whether the DHCP snooping function is enabled.

【Configuration Example]】1: The following is an example of enabling the global function switch of DHCP snooping:

```
AC-FS# configure terminal AC-
FS(config)# ip dhcp snooping
AC-FS(config)# end
```

【Verification】1: Use the show ip dhcp snooping command to check whether DHCP snooping is enabled or disabled.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.3ip dhcp snooping bootp-bind

Enable DHCP Snooping to support the Bootp binding function.

ip dhcp snooping bootp-bind

Disable DHCP snooping to support Bootp binding.

no ip dhcp snooping bootp-bind

【Parameter Description】 -

【Default Configuration】 This function is disabled by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 By default, the DHCP Snooping function only forwards Bootp packets. After this function is enabled, the DHCP Snooping function snoops on Bootp protocol packets. After the Bootp client successfully applies for an address, DHCP Snooping adds the Bootp user to the static binding database.

【Configuration Example]】 1: The following is an example of enabling DHCP Snooping to support Bootp binding:

```
AC-FS# configure terminal
AC-FS(config)# ip dhcp snooping bootp-bind AC-
FS(config)# end
```

【Verification】 1: Use the show ip dhcp snooping command to check whether DHCP Snooping supports Bootp binding.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

8.4 ip dhcp snooping check-giaddr

Enable DHCP Snooping to support the function of processing relay request packets.

ip dhcp snooping check-giaddr

Disable DHCP snooping to support the processing of Relay Request packets.

no ip dhcp snooping check-giaddr

【Parameter Description】-

【Default Configuration】 This function is disabled by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 After this function is enabled, services that use DHCP Snooping binding entries generated by relay requests, such as IP Source Guard/dot1x authentication, cannot be deployed. Otherwise, users may not be able to access the Internet.

After this function is enabled, ip dhcp snooping verify mac-address cannot be configured, otherwise the DHCP request packets of the relay will be discarded, resulting in the user not being able to obtain the address.

【Configuration Example]】1: The following is an example of enabling DHCP Snooping to support the processing of Relay request packets:

```
AC-FS# configure terminal
AC-FS(config)# ip dhcp snooping check-giaddr AC-
FS(config)# end
```

【Verification】 1: Use the show run command to check whether DHCP Snooping supports the function of processing Relay request packets.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.5ip dhcp snooping clear-broadcast-flag

Enable DHCP Snooping to clear the broadcast flag.

ip dhcp snooping clear-broadcast-flag

Disable DHCP Snooping to clear the broadcast flag function.

no ip dhcp snooping clear-broadcast-flag

【Parameter Description】 -

【Default Configuration】 This function is disabled by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 After this function is enabled, DHCP Snooping checks the broadcast flag bit of the non-DHCP Relay request message, if the flag bit is set, it will be cleared. The address is set to the broadcast address.

【Configuration Example]】1: The following is an example of enabling DHCP Snooping to support the processing of Relay request packets:

```
AC-FS# configure terminal
AC-FS(config)# ip dhcp snooping clear-broadcast-flag AC-
FS(config)# end
```

【Verification】1: Use the show run command to check whether DHCP Snooping has enabled the function of clearing the broadcast flag.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.6ip dhcp snooping database write-delay

Regularly write all dynamic user information in the DHCP Snooping database to FLASH.

ip dhcp snooping database write-delay time

Turn off the timing write FLASH function.

no ip dhcp snooping database write-delay

【Parameter Description】

Parameter	Description
time	The period of saving database records in seconds, the value range is 600~86400.

【Default Configuration】 This function is disabled by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 By configuring this command, you can write the DHCP Snooping database into the FLASH file. It can prevent the user information from being lost after the device is restarted, so that the user must obtain the IP address again to communicate normally.
Too fast saving frequency will reduce the life of flash.

【Configuration Example]】1: The following is an example of configuring the switch to write the flash at a regular interval of 3600:

```
AC-FS# configure terminal
AC-FS(config)# ip dhcp snooping database write-delay 3600 AC-
FS(config)# end
```

【Verification】 1: Use the show ip dhcp snooping command to view the current recording interval.

【Prompt Information】-

【Common Mistake】 1: The set period value is not within the limited range.

【Platform Description】 -

8.7ip dhcp snooping database write-to-flash

Configure the device to write the dynamic user information of the DHCP Snooping database into the FLASH file in real time.
ip dhcp snooping database write-to-flash

【Parameter Description】-

【Default Configuration】-

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 By executing this command, the dynamic user information in the DHCP Snooping database can be written to the FLASH file in real time.

【Configuration Example]】1: The following is an example of writing the dynamic user information of the DHCP binding database to flash in real time:

```
AC-FS# configure terminal
AC-FS(config)# ip dhcp snooping database write-to-flash AC-
FS(config)# end
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.8ip dhcp snooping information option

Set the option82 option in the DHCP request message.

ip dhcp snooping information option [standard-format]

Cancel the option82 option in the DHCP request message.

no ip dhcp snooping information option [standard-format]

【Parameter Description】

Parameter	Description
standard-format	Option82 options use the standard format.

【Default Configuration】 This function is disabled by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】1: By configuring this command, option82 information will be added to the DHCP request message, and the DHCP server will perform more reasonable address allocation according to the option82 option information.

2: When the option82 option function is enabled, the function is in extended mode by default.

The DHCP Snooping option82 function and the DHCP Relay option82 function cannot be shared.

【Configuration Example]】1: The following is an example of configuring the function of adding option82 to the DHCP request message:

```
AC-FS# configure terminal
AC-FS(config)# ip dhcp snooping information option AC-FS(config)#
end
```

【Verification】1: Use the show ip dhcp snooping command to check whether the Option82 function is enabled or disabled.

【Prompt Information】-

【Common Mistake】1: Enable at the same time as option82 of DHCP Relay. It will cause the option82 Field value in the final DHCP packet to be incorrect.

【Platform Description】 -

8.9ip dhcp snooping information option format remote-id

When the option82 option is set in extended mode, the suboption remote-id is a custom string or hostname.

ip dhcp snooping information option format remote-id { string ascii-string | hostname }

Unset the option82 option's suboption remote-id to a custom string or hostname.

no ip dhcp snooping information option format remote-id { string ascii-string | hostname }

【Parameter Description】-

【Default Configuration】 This function is disabled by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 By configuring this command, when the DHCP message option82 option function is enabled and in the extended mode, the sub-options in the option82 option will be changed.

remote-id is set to custom content.

【Configuration Example]】1: The following configuration is an example of adding the option82 option remote-id to the DHCP request message, and the content is the host name:

【Verification】1: Use the show ip dhcp snooping command to view the Option82 option format.

【Prompt Information】 1: When the command Parameter ascii-string exceeds the limit of 63 characters, it will prompt an error.

% Failed to execute command, because of "Remote-ID string cannot exceed 63 characters".

【Common Mistake】-

【Platform Description】 -

8.10ip dhcp snooping monitor

Enable the global DHCP snooping monitoring function.

ip dhcp snooping monitor

Disable the global DHCP snooping monitoring function.

no ip dhcp snooping monitor

【Parameter Description】 -

【Default Configuration】 This function is disabled by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 After enabling the DHCP snooping monitoring function, it only copies DHCP packets and generates binding entries based on the interaction, but does not check the validity of the packets.

The DHCP snooping monitoring function and the DHCP snooping function are mutually exclusive, and only one of them can be configured.

When the DHCP snooping monitoring function is enabled, for the binding table entry generated by the routing port, when show ip dhcp snooping binding is displayed, the VLAN Field is displayed as 0, indicating that there is no VLAN information.

【Configuration Example]】1: The following is an example of enabling the DHCP snooping monitoring function switch:

```
AC-FS# configure terminal AC-FS(config)#
ip dhcp snooping monitor
AC-FS(config)# end
```

【Verification】1: Use the show run command to check whether DHCP Snooping monitoring is enabled or disabled.

【Prompt Information】 1: If the DHCP Snooping function is enabled globally, the DHCP Snooping monitoring function cannot be configured.

```
% Failed to execute command, because of "Conflict with DHCP snooping".
```

【Common Mistake】-

【Platform Description】 -

8.11ip dhcp snooping suppression

Set the interface to suppression state and discard all DHCP packets sent to the interface.

ip dhcp snooping suppression

Cancel the interface suppression state.

no ip dhcp snooping suppression

【Parameter Description】-

【Default Configuration】 This function is disabled by default.

【Command Mode】 Interface configuration mode or wireless security configuration mode

【Default Level】 14

【Usage Guide】 1: By configuring this command, all DHCP packets under the UNTRUST interface can be rejected, that is, all users under the interface are prohibited from applying for addresses through DHCP.

2: This command will take effect immediately in the Layer 2 switch port, AP port, and wireless security configuration mode. Configuration will fail on other interfaces.

【Configuration Example]】1: The following is an example of configuring GigabitEthernet 0/2 and WLAN 1 to be in suppression state:

```
AC-FS# configure terminal
AC-FS(config)# interface GigabitEthernet 0/2
AC-FS(config-if-GigabitEthernet 0/2)# ip dhcp snooping suppression
AC-FS(config-if-GigabitEthernet 0/2)# end
```

```
AC-FS# configure terminal AC-
FS(config)# wlansec 1
AC-FS(config-wlansec)# ip dhcp snooping suppression
AC-FS(config-if-wlansec)# end
```

【Verification】 1: Use the show run command to view the packet suppression status configured on the corresponding interface.

【Prompt Information】 1: When configuring on the DHCP TRUST port, it will prompt an error.

% Failed to execute command, because of "Security config conflict".

2: When the wired access is not executed on the Layer 2 switch port, AP port or Layer 2 encapsulation sub-interface, an error will be prompted.

% Failed to execute command, because of "Configure is not supported on current interface".

【Common Mistake】 -

【Platform Description】 -

8.12ip dhcp snooping trust

Configure the DHCP snooping trust status of the interface as TRUST.

ip dhcp snooping trust

Configure the DHCP snooping trust status of the interface as UNTRUST.

no ip dhcp snooping trust

【Parameter Description】 -

【Default Configuration】 By default, all interfaces are UNTRUST interfaces.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 1: By configuring this command, configure the interface connected to the legal DHCP server as the TRUST port. All DHCP response packets received by the TRUST interface are forwarded normally, and all DHCP response packets received by the UNTRUST interface will be discarded.

2: This command will take effect immediately when configured on a Layer 2 switch port, AP port or encapsulated sub-interface. Configuring this command on other interfaces will fail.

Usually, the uplink port, that is, the interface connecting to the trusted DHCP server, is set as the TRUST port.

【Configuration Example]】1: The following is an example of configuring interface GigabitEthernet 0/1 as a TRUST port:

```
AC-FS# configure terminal
AC-FS(config)# interface GigabitEthernet 0/1 AC-FS(config-
if-GigabitEthernet 0/1)# ip dhcp snooping trust AC-FS(config-
if-GigabitEthernet 0/1)# end
```

【Verification】1: Use the show ip dhcp snooping command to view the trust status of the interface.

【Prompt Information】 1: If other access security control options are configured on the interface, it cannot be set as a TRUST interface.

```
% Failed to execute command, because of "Security config conflict".
```

2: When the command is not executed on a layer 2 switch port, AP port or encapsulated sub-interface, an error will be prompted.

```
% Failed to execute command, because of "Configure is not supported on current interface".
```

【Common Mistake】-

【Platform Description】 -

8.13 ip dhcp snooping verify mac-address

Enable the source MAC address verification function.

ip dhcp snooping verify mac-address

Disable the source MAC address verification function.

no ip dhcp snooping verify mac-address

【Parameter Description】 -

【Default Configuration】 This function is disabled by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 The source MAC address check function is to check the DHCP request message from the UNTRUST interface to check whether the source MAC address of the link layer header and the CLIENT MAC Field in the DHCP message are the same. When the source MAC address verification fails, the packet will be discarded.

【Configuration Example]】1: The following is an example of opening the source MAC check of DHCP packets:

```
AC-FS# configure terminal
AC-FS(config)# ip dhcp snooping verify mac-address AC-FS(config)#
end
```

【Verification】1: Use the show ip dhcp snooping command to check whether the function is enabled.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.14ip dhcp snooping vlan

Enable DHCP Snooping on the specified VLAN.

ip dhcp snooping vlan { vlan-rng | { vlan-min [vlan-max] } }

Disable the DHCP Snooping function on the corresponding VLAN.

no ip dhcp snooping vlan { vlan-rng | { vlan-min [vlan-max] } }

【Parameter Description】

Parameter	Description
vlan-rng	The vlan range for which dhcp snooping function is in effect.
vlan-min	The lower limit of the vlan for which dhcp snooping function is in effect.

vlan-max	The upper limit of the vlan for which dhcp snooping function is in effect.

【Default Configuration】 By default, after the global DHCP snooping function is enabled, the DHCP snooping function will be enabled on all VLANs.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 By configuring this command, the DHCP snooping function will be enabled in the specified VLAN, and the DHCP snooping function of the specified VLAN can also be disabled. This function must take effect after the global switch of DHCP Snooping is turned on.

【Configuration Example]】 1: The following is an example of enabling DHCP Snooping on VLAN1000:

```
AC-FS# configure terminal
AC-FS(config)# ip dhcp snooping vlan 1000 AC-
FS(config)# end
```

2: The following is an example of enabling DHCP Snooping on VLAN1 to VLAN10:

```
AC-FS# configure terminal
AC-FS(config)# ip dhcp snooping vlan 1-10 AC-
FS(config)# end
```

【Verification】 1: Use the show run command to check which VLANs are in shutdown mode.

【Prompt Information】 1: If the set VLAN value is not within the range of 1~4094, it will prompt an error.

```
% Failed to execute command, because of "Not supported vlan range".
```

2: If the specified VLAN does not exist, an error will be prompted.

```
% Failed to execute command, because of "VLAN not exist".
```

【Common Mistake】 -

【Platform Description】 -

8.15ip dhcp snooping vlan vlan-id information option change-vlan-to vlan

When option82 is set in extended mode, the VLAN in sub-option circuit-id is the specified VLAN.

ip dhcp snooping vlan vlan-id information option change-vlan-to vlan vlan-id

Turn this feature off.

no ip dhcp snooping vlan vlan-id information option change-vlan-to vlan vlan-id

【Parameter Description】

Parameter	Description
vlan-id	Specify the VLAN number to be replaced.

【Default Configuration】 This function is disabled by default.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 By configuring this command, when the option 82 option function of the DHCP message is enabled and in the extended mode, the VLAN filled with the circuit-id sub-option of option 82 is changed to the specified VLAN.

【Configuration Example]】 1: The following is an example of adding option82 to the DHCP request message, where VLAN4094 in the sub-option circuit-id of option82 is modified to VLAN4093:

```
AC-FS# configure terminal
AC-FS(config)# interface GigabitEthernet 0/1
AC-FS(config-if-GigabitEthernet 0/1)# ip dhcp snooping vlan 4094 information option change-vlan-to vlan
4093
AC-FS(config-if-GigabitEthernet 0/1)# end
```

【Verification】 1: Use the show run command to check whether the function is enabled.

【Prompt Information】 1: If the specified VLAN does not exist, it will prompt an error.

```
% Failed to execute command, because of "VLAN not exist".
```

【Common Mistake】 -

【Platform Description】 -

8.16ip dhcp snooping vlan vlan-id information option format-type circuit-id string

When the option82 option is set in extended mode, the sub-option circuit-id is user-defined content (storage format is ASCII) and forwarded.

ip dhcp snooping vlan vlan-id information option format-type circuit-id string ascii-string

Turn off this feature.

no ip dhcp snooping vlan vlan-id information option format-type circuit-id string ascii-string

【Parameter Description】

Parameter	Description
vlan-id	VLAN where the DHCP request message is located.
ascii-string	Circuit ID User-defined content to be populated.

【Default Configuration】 This function is disabled by default.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 By configuring this command, when the option82 option function of the DHCP message is enabled and in the extended mode, the sub-option circuit-id content of option82 is set to the user-defined content. The content is a string of length 3 to 63 bytes.

【Configuration Example】】 1: The following is an example of adding the option82 option to the DHCP request message, where the sub-option circuit-id of option82 contains port-name:

```
AC-FS# configure terminal
AC-FS(config)# interface GigabitEthernet 0/1
AC-FS(config-if-GigabitEthernet 0/1)# ip dhcp snooping vlan 4094 information option format-type
circuit-id string port-name
AC-FS(config-if-GigabitEthernet 0/1)# end
```

【Verification】1: Use the show run command to check whether the function is enabled.

【Prompt Information】 1: If the specified VLAN does not exist, it will prompt an error.

```
% Failed to execute command, because of "VLAN not exist".
```

2: If the specified custom string is not 3 to 63 characters, an error will be prompted.

% Failed to execute command, because of "Circuit-ID string must be 3 to 63 characters".

【Common Mistake】-

【Platform Description】 -

8.17ip dhcp snooping vlan max-user

Set the maximum number of binding users allowed under the specified vlan on the interface.

ip dhcp snooping vlan vlan-word max-user user-number

Turn off this feature.

no ip dhcp snooping vlan vlan-word max-user user-number

【Parameter Description】

Parameter	Description
vlan-word	The vlan range in which Function is in effect.
user-number	Maximum number of users allowed.

【Default Configuration】 This function is disabled by default.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 By configuring this command, the bound user restriction based on interface and VLAN can be enabled, and the corresponding network topology can be used to prevent attacks from forged DHCP packets.

【Configuration Example]】1: The following is to configure the limit on the number of bound users on VLAN 1~10 and VLAN 20 of interface 1, and a maximum of 30 users are allowed:

```
AC-FS# configure terminal
AC-FS(config)# interface GigabitEthernet 0/1
AC-FS(config-if-GigabitEthernet 0/1)# ip dhcp snooping vlan 1-10,20 max-user 30
AC-FS(config-if-GigabitEthernet 0/1)# end
```

【Verification】1: Use the show run command to check whether the function is enabled.

【Prompt Information】 1: If the interface is a DHCP snooping TRUST port, it will prompt an error.

```
% Failed to execute command, because of "Security configuration conflict in interface GigabitEthernet 0/1".
```

2: If the number of bindings generated on the specified interface VLAN is greater than the maximum number of users configured in the command, an error will be prompted.

```
% Failed to execute command, because of "New max address number little more than the current".
```

【Common Mistake】-

【Platform Description】 -

8.18 renew ip dhcp snooping database

Manually import the information in the current flash into the DHCP Snooping binding database.

renew ip dhcp snooping database

【Parameter Description】-

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 By executing this command, the flash file information can be imported into the DHCP Snooping database in real time.

Records in the file whose leases have expired are ignored.

Only add records that do not exist in the current database.

【Configuration Example]】1: The following is an example of importing the flash file information into the DHCP Snooping database:

```
AC-FS# renew ip dhcp snooping database
```

【Verification】1: Use the command show ip dhcp snooping binding to check whether the record is imported.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.19 show ip dhcp snooping

To view the current configuration of DHCP Snooping, you need to execute this command in privileged mode.

show ip dhcp snooping

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Run this command to view the current DHCP Snooping configuration.

【Configuration Example]】1: The following is an example of viewing the current DHCP Snooping configuration:

```
AC-FS# show ip dhcp snooping
Switch DHCP snooping  status                    :   ENABLE
DHCP snooping  Verification of hwaddr status    :   DISABLE
DHCP snooping database write-delay time         : 0 seconds
DHCP snooping option 82 status                  :   DISABLE
DHCP snooping Support bootp bind status         :  DISABLE

Interface                                         Trusted            Rate limit(pps)
_______________________                           ________________   ________________

GigabitEthernet 0/4                               YES                unlimited
Default                                           No
```

Field Description:

Field	Description
Switch DHCP snooping status	Whether the global DHCP Snooping Function of the device is enabled.
Verification of hwaddr field status	DHCP snooping message source mac Check the switch status.
DHCP snooping database write-delay time	Timed write interval for flash.

DHCP snooping option 82 status	Whether to add the option82 option to the DHCP request message.
DHCP snooping Support Bootp bind status	Whether to turn on DHCP Snooping support for Bootp binding Function.
Interface	Interface name.
Trusted	Whether the interface is a TRUST port.
Rate limit	Whether the global DHCP Snooping Function of the device is enabled.

【Prompt Information】-

【Platform Description】 -

8.20show ip dhcp snooping binding

View user information in the DHCP Snooping database.

show ip dhcp snooping binding

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Run this command to view all user information in the current DHCP Snooping database.

【Configuration Example]】1: The following is a display example:

```
AC-FS# show ip dhcp snooping binding
Total number of bindings: 1
NO.    MACADDRESS          IPADDRESS       LEASE(SEC)    TYPE           VLAN  INTERFACE
-----  ------------------  --------------  ------------  -------------  ----  --------------------
1      0000.0000.0001      1.1.1.1         78128         dhcp-snooping  1     GigabitEthernet 0/1
2      0000.0000.0002..... 2.2.2.2         78111         dhcp-snooping  1     WLAN 1
```

Field Description:

Field	Description
Total number of bindings	The number of bindings in the current DHCP Snooping Binding database.
NO.	Record Serial Number
MacAddress	User MAC address.
IpAddress	User IP address.

Lease(sec)	Record lease time.
Type	Record type.
VLAN	VLAN to which the user belongs.
Interface	User's connection port, wired access interface or wireless access WLAN

【Prompt Information】-

【Platform Description】 -

9 IP Source Guard

9.1ip source binding

Add static user information to the IP source address binding database.

ip source binding mac-address vlan vlan-id ip-address { interface interface-id | wlan wlan-id | ip-mac | ip-only }

Delete the corresponding static user.

no ip source binding mac-address vlan vlan-id ip-address { interface interface-id | wlan wlan-id | ip-mac | ip-only }

【Parameter Description】

Parameter	Description
mac-address	The MAC address of the statically added user.
vlan-id	VLAN ID of the statically added user.
ip-address	The IP address of the statically added user.
interface-id	The wired access port to which the statically added user belongs.
wlan wlan-id	The none line of the statically added user is connected to WLAN.
ip-mac	The type of global binding is IP + MAC binding.
ip-only	The type of global binding is IP only binding.

【Default Configuration】 No static user address is added.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 1: By configuring this command, you can allow some users to pass the detection of IP Source Guard, without the need for unified control through DHCP.

2: This command is only supported on wired access Layer 2 switch ports, AP ports, encapsulated sub-interfaces or wireless access WLANs. Other types of ports will fail to configure.

3: By configuring global binding user records, some users can pass IP Source Guard detection on all ports.

4: In the wireless thin AP environment, it is not supported to add the wired port of the wireless AP to the AC to access user static information.

A configured binding record takes effect either on the wired access interface, on the wireless access WLAN, or globally.

For the same user record, the new record will overwrite the properties of the old record.

【Configuration Example]】1: The following is an example of setting and configuring a static user to a wired switch port or wireless WLAN:

AC-FS# configure terminal

```
AC-FS(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 interface GigabitEthernet 0/1 AC-
FS(config)# ip source binding 0000.0000.0002 vlan 1 1.1.1.2 wlan 1
AC-FS(config)# end
```

2: The following is an example of setting a static user to take effect globally, and the filter type is IP+MAC binding:

```
AC-FS# configure terminal
AC-FS(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 ip-mac AC-
FS(config)# end
```

3: The following is an example of setting a static user to take effect globally, and the filter type is only IP binding:

```
AC-FS# configure terminal
AC-FS(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 ip-only AC-
FS(config)# end
```

【Verification】1: Use the show ip source binding command to view the IP source address binding database.

【Prompt Information】 1: When using the no command to delete the static configuration, if the input Parameter is inconsistent with the Parameter in the previous configuration, an error will be prompted.

```
% Failed to execute command, because of "No such binding entry
[mac 0000.0000.0001 ip 1.1.1.1 vlan 2  GLOBAL]".
```

2: When configuring user records, if the entered VLAN does not exist, an error will be prompted.

```
% Failed to execute command, because of "VLAN 4094 not exist".
```

3: When configuring user records, if the input wired interface is not a Layer 2 switch port, AP port or encapsulated sub-interface, an error will be prompted.

```
% Failed to execute command, because of "Configure is not supported on current interface".
```

【Common Mistake】-

【Platform Description】 -

9.2ip verify source

Turn on the IP Source Guard feature on the port.

ip verify source [port-security]

Turn off the IP Source Guard feature on the port.

no ip verify source

【Parameter Description】

Parameter	Description
port-security	Configure IP Source Guard Function for IP+MAC based detection.

【Default Configuration】 This function is disabled by default.

【Command Mode】 Interface configuration mode, wireless security configuration mode or wireless ap-config all configuration mode

【Default Level】 14

【Usage Guide】 1: Use this command to open the IP Source Guard function of the port, and you can perform IP-based detection or IP+MAC-based detection for users.

2: This command is only supported on wired access Layer 2 switch ports, AP ports, encapsulated sub-interfaces, and wireless access WLANs. Configuration will fail on other types of interfaces.

3: Turning on the IP Source Guard function in the wireless ap-config all mode is equivalent to turning on the IP Source Guard function on the wired ports of all APs.

Currently, the number of legitimate users that the IP Source Gourd function of FS devices relies on comes from DHCP Snooping and static user configuration. If only the IP Source Gourd function is enabled on the port, but no legal data source is configured, users connected to the port will not be able to use the network normally.

【Configuration Example]】1: The following is to configure the IP Source Guard function on the wired switch port and wireless WLAN, and only perform IP-based detection on users:

```
AC-FS# configure terminal
AC-FS(config)# interface GigabitEthernet 0/1 AC-
FS(config-if-GigabitEthernet 0/1)# ip verify source AC-
FS(config-if)# end
AC-FS(config)# wlansec 1
AC-FS(config-wlansec)# ip verify source
AC-FS(config-wlansec)# end
```

2: The following is to configure the IP Source Guard function on interface 2 to detect users based on IP+MAC:

```
AC-FS# configure terminal
AC-FS(config)# interface GigabitEthernet 0/2
AC-FS(config-if-GigabitEthernet 0/2)# ip verify source port-security
AC-FS(config-if)# end
AC-FS(config)# wlansec 2
AC-FS(config-wlansec)# ip verify source port-security
AC-FS(config-wlansec)# end
```

【Verification】 1: Use the show ip source binding command to view the IP Source Guard user filtering entries.

2: Use the show run command to check whether the command is configured successfully.

【Prompt Information】 1: If the operation is performed on the DHCP trusted port, it will prompt an error.

```
% Failed to execute command, because of "Security configuration conflict in interface name".
```

【Common Mistake】 1: Enable IP Source Gourd without configuring the source of legal user records.

【Platform Description】 -

9.3 Ip verify source exclude-vlan

Specifies the exception VLAN feature of IP Source Guard on the port.

ip verify source exclude-vlan vlan-id

Removes the exception VLAN feature for IP Source Guard on the port.

no ip verify source exclude-vlan vlan-id

【Parameter Description】

Parameter	Description
vlan-id	The vlan id not controlled by IP Source Guard on the port.

【Default Configuration】 This function is disabled by default.

【Command Mode】 Interface configuration mode or wireless security configuration mode

【Default Level】 14

【Usage Guide】 1: On the port where IP Source Guard is enabled, this command can control some VLANs of the port that are not controlled by IP Source Guard, and the IP packets within these VLANs are not checked and filtered but are directly passed.

2: After IP Source Guard is disabled on the port, the specified exception VLAN will also be automatically cleared.

3: Support configuration under the wired access Layer 2 switch port, AP port, encapsulation sub-interface or wireless access WLAN.

IP Source Guard must be enabled on the interface before specifying the exception VLAN.

【Configuration Example]】1: The following is to configure the IP Source Guard function on the port and specify the exception VLAN:

```
AC-FS# configure terminal
AC-FS(config)# interface GigabitEthernet 0/1 AC-
FS(config-if-GigabitEthernet 0/1)# ip verify source
AC-FS(config-if-GigabitEthernet 0/1)# ip verify exclude-vlan 1
AC-FS(config-if)# end
AC-FS(config)# wlansec 1
AC-FS(config-wlansec)# ip verify source AC-
FS(config-wlansec)# ip verify exclude-vlan 1 AC-
FS(config-wlansec)# end
```

【Verification】1: Use the show run command to check whether the command is configured successfully.

【Prompt Information】 -

【Common Mistake】-

【Platform Description】 -

9.4 show ip source binding

View information about the IP source address binding database.

show ip source binding [ip-address] [mac-address] [dhcp-snooping] [static] [vlan vlan-id] [interface interface-id] [wlan wlan-id]

【Parameter Description】

Parameter	Description
ip-address	Displays the user binding information for the corresponding ip.
mac-address	Displaying user binding information corresponding to mac.
dhcp-snooping	displaying binding information for dynamic users.
static	Displaying static user binding information.

vlan-id	Displaying user binding information corresponding to vlan.
interface-id	Display the user binding information corresponding to wired access interface.
wlan-id	Displays the user binding information of the corresponding None wire access WLAN.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Execute this command to view the configuration of the current IP source address binding database.

【Configuration Example]】 1: The following is a display example:

```
AC-FS# show ip source binding static AC-
FS#show ip source binding static Total
number of bindings: 5
NO.    MACADDRESS          IPADDRESS       LEASE(SEC)    TYPE          VLAN  INTERFACE
------ ------------------- --------------- ------------- ------------- ----- --------------------
1      0001.0002.0001      1.2.3.2         Infinite      Static        1     Global
2      0001.0002.0002.....1.2.3.3          Infinite      Static        1     GigabitEthernet 0/5
3      0001.0002.0003      1.2.3.4         Infinite      Static        1     Global
4      0001.0002.0004      1.2.3.5         Infinite      Static        1     Global
5      0001.0002.0005      1.2.3.6         Infinite      Static        1     WLAN 1
```

Field Description:

Field	Description
Total number of bindings	Number of bindings in the current Binding database
NO.	Record number
MACADDRESS	User MAC address
IPADDRESS	User IP address
LEASE(SEC)	Record lease time
TYPE	Record type
VLAN	User's VLAN
INTERFACE	Wired interface name or None line WLAN ID

【Prompt Information】 -

【Platform Description】 -

9.5 show ip verify source

View IP Source Guard user filter entries.

show ip verify source [interface interface-id] [wlan wlan-id]

【Parameter Description】

Parameter	Description
interface-id	Displays the user filtering table entries for the corresponding wired interface.
wlan-id	Display the user filtering table entries for the corresponding None line WLAN.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Execute this command to check the effective status of the current IP source address binding user record. The logging states currently supported by IP Source Guard include the following:

1. Inactive-restrict-off, the interface to which the binding record belongs does not have the IP Source Guard function enabled.

2. Inactive-system-error, the bound user record cannot be converted into a filter entry due to a system error.

3. Active, the filter entry corresponding to the bound user record entry has taken effect.

【Configuration Example]】1: The following is a display example:

```
AC-FS # show ip verify source
Total number of bindings: 7
NO.    INTERFACE            FILTERTYPE  FILTERSTATUS           IPADDRESS       MACADDRESS
VLAN TYPE

1         Global                              IP+MAC          Inactive-system-error 192.168.0.127 0001.0002.0003 1
Static
2        GigabitEthernet 0/5  IP-ONLY         Active1.2.3.4                    0001.0002.0004   1
DHCP-Snooping
3        Global                 IP-ONLY          Active1.2.3.7                  0001.0002.0007   1 Static
4     Global                  IP+MAC               Active1.2.3.6                  0001.0002.0006   1  Static
5        GigabitEthernet 0/1  UNSET           Inactive-restrict-off  1.2.3.9            0001.0002.0009 1 DHCP-Snooping
6        GigabitEthernet 0/5  IP-ONLY         Active                                  Deny-All
7        WLAN 1                      IP-ONLY        Active                                  Deny-ALL
```

Field Description:

Field	Description
NO.	Record Serial Number.
INTERFACE	Wired access interface or None line access WLAN.
FILTERTYPE	Filtering Policy.
FILTERSTATUS	Status.
IPADDRESS	User IP address.
MACADDRESS	User MAC address.
VLAN	User's VLAN.
TYPE	User type, including DHCP Snooping dynamically generated or statically.

【Prompt Information】-

【Platform Description】 -

10 DNS SNOOPING

10.1 clear free-url

Clear authentication-free URL information.

clear free-url

【Parameter Description】 -

【Command Mode】 Privileged mode, global mode

【Default Level】 14

【Usage Guide】 Use this command to clear the authentication-free URL information.

【Configuration Example]】1: Clear the authentication-free APP information

```
AC-FS(config)#clear free-url
```

【Prompt Information】-

【Platform Description】 -

10.2 free-url

Configure an authentication-free URL.

free-url { weixin | sina | iphone | url url }[wlan wlan-id]

Cancel the authentication-free URL.

no free-url { weixin | sina | iphone | url url }[wlan wlan-id]

【Parameter Description】

Parameter	Description
wechat	WeChat content authentication-free.
sina	No authentication for Sina APP.
iphone	No authentication for iphone specific APP.
url	Authentication-free URL

wlan	WLAN information

【Default Configuration】 The default is empty configuration.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Multiple authentication-free URLs can be opened at the same time.

【Configuration Example]】1: Configure the authentication-free URL.

```
AC-FS#configure terminal AC-
FS(config)# free-url weixin
AC-FS(config)#exit
```

【Verification】1: Use the show free-url command to view the information about the authentication-free URL.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

10.3 ip dns snooping enable

Enable DNS sniffing.

ip dns snooping enable

Turn off DNS sniffing.

no ip dns snooping enable

【Parameter Description】 -

【Default Configuration】Enable.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Use this command to enable DNS sniffing.

【Configuration Example]】1: Disable DNS sniffing.

```
AC-FS#configure terminal AC-FS(config)#no
ip dns snooping enable
AC-FS(config)#exit
```

【Verification】1: Use the show run command to view the configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 Only supports switch products

10.4 show dns snooping statistics

View DNS packet statistics.

show dns snooping statistics

【Parameter Description】-

【Command Mode】 Privileged mode, global mode

【Default Level】 14

【Usage Guide】 Use this command to view DNS packet statistics.

【Configuration Example]】1: View dns packet statistics.

```
AC-FS#show dns snooping statistics
Receive dns request packet counts : 0
Receive dns reply packet counts  : 0
AC-FS#
```

Field Description: -

【Prompt Information】-

【Platform Description】 -

10.5 show free-url

View authentication-free URL information.

show free-url

【Parameter Description】-

【Command Mode】 Privileged mode, global mode

【Default Level】 14

【Usage Guide】 Use this command to view the information about the authentication-free URL.

【Configuration Example]】1: View the information of the authentication-free APP

```
AC-FS(config)#show   free-url
Total number of domain name : 4
Total number of ip address  : 11

======================== free-url domain name table ==========================
Host                    type
*.qpic.cn               weixin
*.weixin.qq.com         weixin
weixin.qq.com           weixin
*.baidu.com             url
==============================================================================

========================== free-url ip table ================================
Host                    type    Address                         TTL(sec)
*.weixin.qq.com         weixin  61.151.224.41                    2118
                                140.207.135.125                 2118
                                140.207.54.47                   2118
*.qpic.cn               weixin  140.206.160.234                 2118

                                183.61.49.180                   151
                                101.226.129.204                 554
                                14.17.52.136                    16
weixin.qq.com           weixin  14.17.42.45                     800
*.baidu.com             url.....115.239.210.246                 19
                                115.239.211.235                 2286
                                115.239.210.14                  284
==============================================================================
```

Field Description:

Field	Description
Host	Domain Name
type	Type
Address	ip address
T L	Survival time

【Prompt Information】-

【Platform Description】 -

11 IGMP Snooping

11.1 clear ip igmp snooping gda-table

Clear dynamic forwarding entries.

clear ip igmp snooping gda-table

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 The IGMP Snooping forwarding entry includes: VLAN number, group address, routing connection port, and member port.

The VLAN number and group address uniquely identify a forwarding entry.

A forwarding entry can contain multiple routing ports (may be dynamic routing ports or static routing ports). Static route connections will not age out.

A forwarding entry can contain multiple member ports (may be dynamic member ports or static member ports). Static member ports do not age out. Static member ports cannot be deleted using the clear ip igmp snooping gda-table command.

【Configuration Example】AC-FS# clear ip igmp snooping gda-table

【Prompt Information】-

【Platform Description】 -

11.2ip igmp snooping

Start IGMP Snooping globally and set the IVGL operating mode.

ip igmp snooping

Turn off IGMP Snooping.

no ip igmp snooping

Restore IGMP Snooping Default Configuration

default ip igmp snooping

【Parameter Description】-

【Default Configuration】 Disable IGMP Snooping.

【Command Mode】 In global mode or AC ap-config mode

【Default Level】 14

【Usage Guide】 ↑ In IVGL mode, the multicast streams between VLANs are independent of each other. A host can only request to receive a multicast stream from the routing interface that is in the same VLAN as itself; when a device receives a multicast stream from any VLAN, it can only forward it to the member ports in the same VLAN. On the AC, run the igmp snooping command in the ap-config mode to enable the AP's multicast function, and use no igmp snooping to disable the AP's multicast function.

【Configuration Example】1: Enable IGMP Snooping IVGL mode.

```
AC-FS(config)# ip igmp snooping ivgl
```

【Verification】View the current IGMP Snooping status through the show ip igmp snooping command

【Prompt Information】 1: If the device does not support IVGL mode, it will prompt an error.

```
% Error: It's invalid to configure IVGL mode in this product.
```

2: If the device is configured with Layer 2 multicast static flow control, it will prompt to disable Layer 2 multicast static flow control first.

```
% Error: IGMP Snooping conflicts with ip multicast static rule, please disable ip multicast static
rule and try again.
```

【Common Mistake】-

【Platform Description】 -

11.3ip igmp snooping fast-leave enable

Enable the port quick leave feature.

ip igmp snooping fast-leave enable

Disable the port quick leave function.

no ip igmp snooping fast-leave enable

Restore Quickaway Default Configuration

default ip igmp snooping fast-leave enable

【Parameter Description】-

【Default Configuration】 Disable this function

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 After enabling the port quick leave function, when a port of the device receives a Leave message, it will directly delete the port from the member port of the corresponding forwarding entry. After that, when the device receives the corresponding specific group query message, the device no longer forwards it to the port. Among them, the Leave message includes the Leave message of IGMPv2 and the Report message of the include type in IGMPv3 and without any source address.

The port quick leave function is only applicable to the case where only one host is connected to one port of the device, which can save bandwidth and resources.

【Configuration Example】1: Enable port quick leave function

```
AC-FS(config)# ip igmp snooping fast-leave
```

【Verification】View the current configuration Parameter through the show ip igmp snooping command.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

11.4 ip igmp snooping host-aging-time

Configure the aging time of IGMP dynamic member ports.

ip igmp snooping host-aging-time seconds

Delete the IGMP dynamic member port aging time configuration.

no ip igmp snooping host-aging-time

Restore the default value of the aging time of IGMP dynamic member ports.

default ip igmp snooping host-aging-time

【Parameter Description】

Parameter	Description
seconds	Aging time. The unit is seconds and the value range is 1-65535.

【Default Configuration】 260 seconds.

【Command Mode】 Global mode or AC ap-config mode

【Default Level】 14

【Usage Guide】 Dynamic member port aging time refers to the aging time set for this dynamic member port when a port of the device receives an IGMP join packet sent by a host to join an IP multicast group.

After receiving the IGMP join message, the aging timer of this dynamic member port will be reset, and the timer time is host-aging-time. If the timer expires, it is considered that there is no user host receiving multicast packets under the port, and the multicast device will delete the port from the member ports of IGMP Snooping. After this command is configured, the value of the dynamic member port aging timer is set to host-aging-time when the IGMP join message received later is set. This configuration takes effect the next time a join packet is received, and the timers of the currently activated member ports will not be updated.

In the ap-config mode of the AC, run the igmp snooping host-aging-time seconds command to configure the AP member aging time, and run the no igmp snooping host-aging-time command to restore the default member aging time.

【Configuration Example]】1: Configure the IGMP dynamic port aging time to 30s.

```
AC-FS(config)# ip igmp snooping host-aging-time 30
```

【Verification】View the configured Parameter through show ip igmp snooping

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

11.5ip igmp snooping ignore-query-timer

Configure ignoring query packets to reset the port aging timer.

ip igmp snooping ignore-query-timer

Delete ignore query packets and reset port aging timer.

no ip igmp snooping ignore-query-timer

Restore the default value of the aging time of IGMP dynamic member ports.

default ip igmp snooping ignore-query-timer

【Parameter Description】-

【Default Configuration】 By default, the port aging timer is reset without ignoring query packets.

【Command Mode】 Global mode or AC ap-config mode

【Default Level】 14

【Usage Guide】 1. This command is an optimization command. In a wireless environment, you can configure this command when the network environment is not stable. Due to the possibility of packet loss, if the report packet received in response to the query packet is lost. , the port will age out quickly.

2. In the ap-config mode of the AC, run the igmp snooping ignore-query-timer command to configure the AP to ignore query packets to reset the port aging timer function, and run the no igmp snooping ignore-query-timer to restore the default configuration.

【Configuration Example]】1: Configure ignoring query packets to reset the port aging timer.

```
AC-FS(config)# ip igmp snooping ignore-query-timer
```

【Verification】View the configured Parameter through show ip igmp snooping

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

11.6ip igmp snooping mcast-to-unicast enable

Enable the multicast-to-unicast function.

ip igmp snooping mcast-to-unicast enable

Disable the multicast-to-unicast function.

no ip igmp snooping mcast-to-unicast enable

Restore the Default Configuration of the dynamically learned route connection port.

default ip igmp snooping mcast-to-unicast enable

【Parameter Description】-

【Default Configuration】 This function is not enabled

【Command Mode】ap-config mode on AC or global mode of fat AP

【Default Level】 14

【Usage Guide】 In the wireless multicast environment, only the AP has the function of multicast to unicast.

1. After the multicast-to-unicast function is enabled, when the packet arrives at the AP, the packet can determine which multicast packets need to be converted to unicast for transmission according to the multicast-to-unicast policy.

2. The command in ap-config mode on the AC is igmp snooping mcast-to-unicast enable.

3. Configure no igmp snooping mcast-to-unicast enable in ap-config mode on AC and no ip igmp snooping mcast-to-unicast enable in fat AP global mode to disable multicast to unicast function.

After the multicast-to-unicast function is enabled, only users who meet the multicast-to-unicast policy are allowed to forward multicast packets to unicast. Multicast-to-unicast processing not only requires enabling the multicast-to-unicast command, but also needs to refer to other policies, such as packet rate, multicast-to-unicast range, and so on.

【Configuration Example】1: Enable multicast to unicast function in ap-config mode

```
AC-FS(config-ap)# igmp snooping mcast-to-unicast enable
```

【Verification】Use the show ip igmp snooping command to check whether the configuration takes effect.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

11.7ip igmp snooping mcast-to-unicast group-range

Configure the multicast-to-unicast multicast group range.

ip igmp snooping mcast-to-unicast group-range ip-addr ip-addr

Delete the multicast-to-unicast multicast group range configuration.

no ip igmp snooping mcast-to-unicast group-range

Restore Default Configuration.

default ip igmp snooping mcast-to-unicast group-range

【Parameter Description】

Parameter	Description
ip-addr	Broadcast address, range 224.0.1.0 to 239.255.255.255.

【Default Configuration】 The multicast group range is not configured, all legal multicast addresses allow multicast to unicast.

【Command Mode】ap-config mode on AC or global mode of fat AP

【Default Level】 14

【Usage Guide】 In the wireless multicast environment, only the AP has the relevant configuration of the multicast-to-unicast function

1. After configuring the range of multicast-to-unicast multicast group, the bandwidth can be used reasonably, and the multicast groups that need to be converted to unicast can be converted to unicast and forwarded, and the multicast groups that do not need to be converted to unicast and forwarded can still be forwarded. Multicast forwarding.

2. The command in ap-config mode on the AC is igmp snooping mcast-to-unicast group-range.

3. Configure no igmp snooping mcast-to-unicast group-range in ap-config mode on the AC and configure no ip igmp snooping mcast-to-unicast group-range in fat AP global mode to restore the default configuration.

【Configuration Example]】1: Configure the range of multicast-to-unicast multicast groups in ap-config mode.

```
AC-FS(config-ap)# igmp snooping mcast-to-unicast group-range 239.1.1.1. 239.10.1.1.1
```

【Verification】Use the show ip igmp snooping command to check whether the configuration takes effect.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

11.8ip igmp snooping mcast-to-unicast max-group

Configure the maximum number of groups to convert from multicast to unicast.

ip igmp snooping mcast-to-unicast max-group number

Delete the configuration of the maximum number of groups from multicast to unicast.

no ip igmp snooping mcast-to-unicast max-group

Restore Default Configuration.

default ip igmp snooping mcast-to-unicast max-group

【Parameter Description】

Parameter	Description
number	The maximum number of multicast transferred to unicast, ranging from 1 to 64.

【Default Configuration】 The default value is 64

【Command Mode】ap-config mode on AC or global mode of fat AP

【Default Level】 14

【Usage Guide】 In the wireless multicast environment, only the AP has the relevant configuration of the multicast-to-unicast function

1. After configuring the maximum number of multicast-to-unicast groups, the bandwidth can be used reasonably. If the number of configured groups is relatively large, these groups need to be converted to unicast, but the current bandwidth is not enough to support so many groups for unicast conversion, you can use this command to adjust the maximum supported multicast transfer The number of unicasts, so that the bandwidth can be fully utilized. Moreover, when a multicast group exits from multicast to unicast, other groups can join the multicast to convert to unicast, which can control resources more effectively.

2. The command in ap-config mode on the AC is igmp snooping mcast-to-unicast max-group

3. Configure no igmp snooping mcast-to-unicast max-group in ap-config mode on AC and configure in fat AP global mode

default ip igmp snooping mcast-to-unicast max-group can restore the default configuration

【Configuration Example]】1: Configure the maximum number of groups from multicast to unicast in ap-config mode

```
AC-FS(config-ap)# igmp snooping mcast-to-unicast max-group 10
```

【Verification】Use the show ip igmp snooping command to check whether the configuration takes effect

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

11.9ip igmp snooping mrouter learn pim-dvmrp

Enable the function of dynamically learning the route connection interface.

ip igmp snooping [vlan vid] mrouter learn pim-dvmrp

Disable the function of dynamically learning routing connections.

no ip igmp snooping [vlan vid] mrouter learn pim-dvmrp

Restore the Default Configuration of the dynamically learned route connection port.

default ip igmp snooping [vlan vid] mrouter learn pim-dvmrp

【Parameter Description】

Parameter	Description
vlan vid	The default applies to all vlan.

【Default Configuration】 Enable this function

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 The routing connection port is the port on the multicast device with IGMP Snooping enabled that is directly connected to the multicast neighbor device with the multicast routing protocol enabled. By default, the function of dynamically learning routing ports is enabled, and the device automatically listens to IGMP Query/DVMRP/PIM Hello packets to dynamically identify routing ports.

1. Enable the function of dynamically learning the routing connection port (enabled by default), you can obtain the dynamic routing connection port.

2. Configure the ip igmp snooping vlan mrouter interface command to get the static route connection port.

3. Configure the no ip igmp snooping mrouter learn pim-dvmrp command, and disable the function of dynamically learning routing interfaces for all VLANs.

4. Configure the no ip igmp snooping vlan vid mrouter learn pim-dvmrp command to disable the function of dynamically learning the routing interface only for a single VLAN.

When the source port check function is enabled, only the multicast stream entering from the routing port is legal, and the multicast device forwards the data stream to the registered port; the multicast stream entering from the non-routing port is regarded as a valid port. Illegal and will be discarded.

【Configuration Example]】1: Only enable the function of dynamically learning the routing interface on VLAN1.

```
AC-FS(config)# no ip igmp snooping mrouter learn pim-dvmrp
AC-FS(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
```

【Verification】View Parameter through the show ip igmp snooping command.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

11.10ip igmp snooping querier

Enable the IGMP Snooping querier function.

ip igmp snooping [vlan vid] querier

Disable the IGMP Snooping querier function.

no ip igmp snooping [vlan vid] querier

Restore Default Configuration.

default ip igmp snooping [vlan vid] querier

【Parameter Description】

Parameter	Description
vlan vid	The default applies to all vlan.

【Default Configuration】 Disable this function.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 After the querier function is enabled globally, and then enable the querier function on the VLAN, the querier function on the VLAN can take effect. If the querier function is turned off globally, the querier function on all VLANs will be turned off.

【Configuration Example】1: Enable the querier function on VLAN2.

```
AC-FS(config)# ip igmp snooping querier
AC-FS(config)# ip igmp snooping vlan 2 querier
```

【Verification】 Use the show ip igmp snooping querier or show ip igmp snooping querier detail command to view the status and Parameter information of the querier

【Prompt Information】 1: Before configuring the global querier, configure the querier function of the VLAN, and an error message will be displayed

```
% Command did not take effect due to reason: IGMP switch querier is globally disabled
```

【Common Mistake】 1: Before the global querier function is enabled, enable the VLAN querier function first, and the VLAN querier function cannot be configured at this time.

【Platform Description】 -

11.11ip igmp snooping querier address

Configure the source IP address of the IGMP Snooping querier.

ip igmp snooping [vlan vid] querier address a.b.c.d

Delete configuration.

no ip igmp snooping [vlan vid] querier address

Restore Default Configuration.

default ip igmp snooping [vlan vid] querier address

【Parameter Description】

Parameter	Description
vlan vid	The default applies to all vlan.
a.b.c.d	Source IP address.

【Default Configuration】-

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 After enabling the querier function, you must specify a source IP address for the querier, otherwise the querier function will not take effect. If the querier's source IP address is specified on the VLAN, the configuration on the VLAN takes precedence.

【Configuration Example]】1: Configure the source IP address of the IGMP Snooping querier as 1.1.1.1.

```
AC-FS(config)# ip igmp snooping querier address 1.1.1.1
```

2: Configure the source IP address of the IGMP Snooping querier on VLAN3 as 1.1.1.1.

```
AC-FS(config)# ip igmp snooping vlan 3 querier address 1.1.1.1
```

【Verification】 Use the show ip igmp snooping querier or show ip igmp snooping querier detail command to view the status and Parameter information of the querier

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

11.12ip igmp snooping querier max-response-time

Configure the maximum response time of the IGMP Snooping querier.

ip igmp snooping [vlan vid] querier max-response-time seconds

Delete configuration.

no ip igmp snooping [vlan vid] querier max-response-time

Restore default values.

default ip igmp snooping [vlan vid] querier max-response-time

【Parameter Description】

Parameter	Description
vlan vid	The default applies to all vlan.
seconds	Maximum response time. The unit is seconds, and the value range is 1-25.

【Default Configuration】10 seconds.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 If the maximum response time of the querier is specified on the VLAN, the configuration on the VLAN will be used first.

【Configuration Example]】1: The maximum response time of the configuration querier is 15 seconds.

```
AC-FS(config)# ip igmp snooping querier max-response-time 15
```

2: Configure the maximum response time of the querier for VLAN3 to be 15 seconds.

```
AC-FS(config)# ip igmp snooping vlan 3 querier max-response-time 15
```

【Verification】Use the show ip igmp snooping querier or show ip igmp snooping querier detail command to view the status and Parameter information of the querier.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

11.13 ip igmp snooping querier query-interval

Configure the query interval of the IGMP Snooping querier.

ip igmp snooping [vlan vid] querier query-interval seconds

delete configuration

no ip igmp snooping [vlan vid] querier query-interval

Restore default values.

default ip igmp snooping [vlan vid] querier query-interval

【Parameter Description】

Parameter	Description
vlan vid	Specify VLAN. The default applies to all VLANs.
seconds	Query interval. The unit is seconds, and the value range is 1-18000.

【Default Configuration】 60 seconds

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 If the query interval is specified on the VLAN, the configuration on the VLAN will be used first.

【Configuration Example]】1: Configure the query interval.

```
AC-FS(config)# ip igmp snooping querier query-interval 100
```

2: Configure the query interval for a single VLAN.

```
AC-FS(config)# ip igmp snooping vlan 3 querier query-interval 100
```

【Verification】 Use the show ip igmp snooping querier or show ip igmp snooping querier detail command to view the status and Parameter information of the querier

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

11.14ip igmp snooping querier timer expiry

Configure the timeout period of the IGMP Snooping querier.

ip igmp snooping [vlan vid] querier timer expiry seconds

Delete configuration.

no ip igmp snooping [vlan vid] querier timer expiry

Restore default values.

default ip igmp snooping [vlan vid] querier timer expiry

【Parameter Description】

Parameter	Description
vlan vid	The default applies to all vlan.
seconds	Timeout time. The unit is seconds, and the value range is 60-300.

【Default Configuration】 125 seconds

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 After enabling the querier function, you may also lose the election. If the loser does not receive the query message sent by the current querier within the "querier timeout period", the current querier is considered invalid and the next round of election is initiated.

If the querier timeout has been configured on the corresponding VLAN, the value configured on the VLAN will be used first.

【Configuration Example]】1: Configure the querier timeout to 60 seconds.

```
AC-FS(config)# ip igmp snooping querier timer expiry 60
```

2: Configure the querier timeout for VLAN3 to be 60 seconds.

```
AC-FS(config)# ip igmp snooping vlan 3 querier timer expiry 60
```

【Verification】Use the show ip igmp snooping querier or show ip igmp snooping querier detail command to view the status and Parameter information of the querier

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

11.15ip igmp snooping querier version

Configure the IGMP Snooping querier to run IGMPv1.

ip igmp snooping [vlan vid] querier version 1

Configure the IGMP Snooping querier to run IGMPv2.

ip igmp snooping [vlan vid] querier version 2

Delete querier version number configuration.

no ip igmp snooping [vlan vid] querier version

Restore Default Configuration.

default ip igmp snooping [vlan vid] querier version

【Parameter Description】

Parameter	Description
vlan vid	The default applies to all vlan.

【Default Configuration】 The IGMP Snooping querier runs IGMPv2.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 The querier supports IGMPv1 or IGMPv2.

If the IGMP version running on the querier has been configured on the VLAN, the configuration on the VLAN takes precedence.

【Configuration Example】1: Set the querier to run IGMPv1.

```
AC-FS(config)# ip igmp snooping querier version 1
```

2: Set the querier of VLAN3 to run IGMPv1.

```
AC-FS(config)# ip igmp snooping vlan 3 querier version 1
```

【Verification】 Use the show ip igmp snooping querier or show ip igmp snooping querier detail command to view the status and Parameter information of the querier

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

11.16 ip igmp snooping query-max-response-time

Configure the maximum response time for query packets.

ip igmp snooping query-max-response-time seconds

Delete configuration.

no ip igmp snooping query-max-response-time

Restore default values.

default ip igmp snooping query-max-response-time

【Parameter Description】

Parameter	Description
seconds	The maximum response time of the query message in seconds, the value range is 1-65535.

【Default Configuration】 10 seconds

【Command Mode】 Global mode or AC ap-config mode

【Default Level】 14

【Usage Guide】 1. After receiving the IGMP general query message, the multicast device will reset the aging timer of all dynamic member ports, and the timer time is query-max-response-time. If the timer expires, it is considered that there is no user host receiving multicast packets under the port, and the multicast device will delete the port from the member ports of IGMP Snooping.

2. After receiving the IGMP specific group query message, the multicast device will reset the aging timer of all dynamic member ports of the specific group, and the timer time is query-max-response-time. If the timer expires, it is considered that there is no user host receiving multicast packets under the port, and the multicast device will delete the port from the member ports of IGMP Snooping.

3. The configuration takes effect the next time a query packet is received, and the currently started timer will not be updated. For IGMPv3 specific group source query packets, no timer update processing is performed.

4. In the ap-config mode of the AC, run the command igmp snooping query-max-response-time seconds to configure the maximum query response time of the AP, and run the no igmp snooping query-max-response-time command to restore the default configuration.

【Configuration Example】1: The maximum response time of configuration query packets is 100s.

```
AC-FS(config)# ip igmp snooping query-max-response-time 100
```

【Verification】Use the show ip igmp snooping querier or show ip igmp snooping querier detail command to view the status and Parameter information of the querier

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

11.17 ipip igmp snooping suppression enable

Enable the suppression of Report packets.

ip igmp snooping suppression enable

Disable the suppression of Report packets.

no ip igmp snooping suppression enable

Restore Default Configuration.

default ip igmp snooping suppression enable

【Parameter Description】-

【Default Configuration】 Disable this function

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 When the report packet suppression function is enabled, only the first received Report packet of a specific vlan and group will be forwarded to the routing interface within a query interval, and subsequent Report packets will not continue to be sent to the routing interface. It is forwarded by the routing connection port, which can reduce the number of packets in the network.
Only the Report message of IGMPv1/v2 can be suppressed, and it is invalid for the Report message of IGMPv3.

【Configuration Example】1: Enable the suppression function of Report message.

```
AC-FS(config)# ip igmp snooping suppression enable
```

【Verification】View the configured Parameter through show ip igmp snooping.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

11.18ip igmp snooping vlan

Enable IGMP Snooping (IVGL mode) on the VLAN.

ip igmp snooping vlan vid

Turn off IGMP Snooping (IVGL mode) on the VLAN.

no ip igmp snooping vlan vid

Restore Default Configuration

default ip igmp snooping vlan vid

【Parameter Description】

【Default Configuration】 If IGMP Snooping (IVGL mode) is enabled globally, all VLANs will enable IGMP Snooping (IVGL mode).

If IGMP Snooping (IVGL mode) is not enabled globally, IGMP Snooping (IVGL mode) is disabled for all VLANs.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 When IGMP Snooping (IVGL mode) is enabled globally, use the no ip igmp snooping vlan vid command to enable IGMP Snooping (IVGL mode) on other VLANs except the specified VLAN.

PIM Snooping must rely on IGMP Snooping. When using no ip igmp snooping vlan to disable the IGMP Snooping function on a VLAN, if PIM Snooping is enabled on the VLAN, the shutdown will fail, and a prompt will be displayed to disable PIM Snooping first.

【Configuration Example]】1: Enable IGMP Snooping (IVGL mode) globally, and disable IGMP Snooping (IVGL mode) on vlan 2.

```
AC-FS(config)# ip igmp snooping ivgl
AC-FS(config)# no ip igmp snooping vlan 2
```

【Verification】View the configured Parameter through show ip igmp snooping vlan.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

11.19ip igmp snooping vlan fast-leave enable

Configure the quick leave function for the specified vlan.

ip igmp snooping vlan vid fast-leave enable

turn off quick leave for vlan

no ip igmp snooping vlan vid fast-leave enable

Restore the default configuration of the quick leave function of vlan

default ip igmp snooping vlan vid fast-leave enable

【Parameter Description】

【Default Configuration】The quick function of vlan is opened

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Enable the quick leave function of vlan (enabled by default)

Run the no ip igmp snooping vlan fast-leave enable command to disable the fast-leave function of the specified vlan.

The fast leave function of vlan needs to be used together with the global configuration ip igmp snooping fast-leave enable. If the global is not turned on, the quick leave function of vlan does not take effect.

【Configuration Example]】1: Disable the vlan quick leave function.

```
AC-FS(config)# no ip igmp snooping vlan 1 fast-leave enable
```

【Verification】View the configured Parameter through show run

【Prompt Information】1: If the quick leave function of vlan is configured and the global quick leave function is not enabled, the Prompt Information

```
% Warning: Please remember to enable global fast leave
```

【Common Mistake】-

【Platform Description】 -

11.20ip igmp snooping vlan mrouter interface

Configure a static route connection port.

ip igmp snooping vlan vid mrouter interface interface-type interface-number

Unconfigure.

no ip igmp snooping vlan vid mrouter interface interface-type interface-number

Restore Default Configuration.

default ip igmp snooping vlan vid mrouter interface interface-type interface-number

【Parameter Description】

Parameter	Description
vid	VLAN number, value range 1-4094.
interface-type interface-number	Interface name.

【Default Configuration】 No static routing port

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 When the function of dynamically learning the route connection port is enabled (enabled by default), the dynamic route connection port can be obtained.

Configure the ip igmp snooping vlan mrouter interface command to obtain the static route connection port. Static route connections will not age out.

If a port is configured as a static route connection port, all multicast streams received on the device can be forwarded through this port.

When the source port check function is enabled, only the multicast stream entering from the routing port is legal, and the device forwards the multicast stream to the registered port; the multicast stream entering from the non-routing port is regarded as illegal. , will be discarded.

【Configuration Example]】 1: Configure a static route connection port.

```
AC-FS(config)# ip igmp snooping vlan 1 mrouter interface fastEthernet 0/1
```

【Verification】 View the configured Parameter through show ip igmp snooping.

【Prompt Information】 1: If the configuration of the static route connection port fails, the Prompt Information.

```
% Error: Configure this interface static multicast route failure
```

【Common Mistake】 -

【Platform Description】 -

11.21ip igmp snooping vlan static interface

Configure static member ports.

ip igmp snooping vlan vid static group-address interface interface-type interface-number

Unconfigure.

no ip igmp snooping vlan vid static group-address interface interface-type interface-number

Restore Default Configuration.

default ip igmp snooping vlan vid static group-address interface interface-type interface-number

【Parameter Description】

Parameter	Description
vid	VLAN number, value range 1-4094.
group-address	Group address.
interface-type interface-number	Interface name.

【Default Configuration】 No static member port

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 The IGMP Snooping forwarding entry includes: VLAN number, group address, routing connection port, and member port.

The VLAN number and group address uniquely identify a forwarding entry.

A forwarding entry can contain multiple routing ports (may be dynamic routing ports or static routing ports). Static route connections will not age out.

A forwarding entry can contain multiple member ports (may be dynamic member ports or static member ports). Static member ports do not age out. Static member ports cannot be deleted using the clear ip igmp snooping gda-table command.

【Configuration Example]】1: Configure GigabitEthernet 0/1 as a static member port of vlan 1 group 224.1.1.1.

```
AC-FS(config)# ip igmp snooping vlan 1 static 224.1.1.1 interface GigabitEthernet 0/1
```

【Verification】View the configured Parameter through show ip igmp snooping

【Prompt Information】 1: If the configuration of the static route connection port fails, the Prompt Information

```
% Error: Configure static multicast group in this port fail
```

【Common Mistake】-

【Platform Description】 -

11.22ip multicast wlan

Enable global multicast state.

ip multicast wlan

Delete configuration.

no ip multicast wlan

Restore Default Configuration.

default ip multicast wlan

【Parameter Description】 -

【Default Configuration】 The global multicast state is not enabled by default

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Only AC and fat AP support this command.

1. When the global multicast state is not enabled, when the AC or fat AP receives the multicast packet, it will be discarded without processing.

2. Configure ip multicast wlan to enable global multicast status

【Configuration Example]】1: Enable global multicast state in global mode.

```
AC-FS(config)# ip multicast wlan
```

【Verification】Use the show ip igmp snooping command to check whether the configuration takes effect.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -Only supported by wireless product platforms.

11.23 show ip igmp snooping

Display various information of IGMP Snooping.

show ip igmp snooping [vlan vid]

Displays the forwarding table for IGMP Snooping.

show ip igmp snooping gda-table

Displays the routing port of IGMP Snooping.

show ip igmp snooping mrouter

Display IGMP Snooping interface query information.

show ip igmp snooping querier [detail | vlan vid]

【Parameter Description】

Parameter	Description
vlan vid	The default is to display information for all VLANs.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to view the IGMP Snooping status and Parameter information of the global or specified VLAN.

【Configuration Example]】1: View global IGMP Snooping information

```
AC-FS#show  ip igmp  snooping
IGMP Snooping running mode: IVGL
IGMP Snooping L2-entry-limit: 65536
Source port check: Disable
Source  ip  check:  Disable
IGMP  Fast-Leave:  Disable
IGMP Report suppress: Disable
IGMP Globle Querier: Disable
IGMP Preview: Disable
IGMP Tunnel: Disable
IGMP Preview group aging time : 60(Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Dynamic Host Aging Time : 260(Seconds)
AC-FS#show  ip igmp  snooping
IGMP Snooping running mode: IVGL
IGMP Snooping L2-entry-limit: 65536
Source port check: Disable
Source  ip  check:  Disable
IGMP  Fast-Leave:  Disable
IGMP Report suppress: Disable
IGMP Globle Querier: Disable
IGMP Preview: Disable
IGMP Tunnel: Disable
IGMP Preview group aging time : 60(Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Dynamic Host Aging Time : 260(Seconds)
```

2: View VLAN1 IGMP Snooping information

```
AC-FS#show ip igmp snooping vlan 1
IGMP Snooping running mode: IVGL
```

```
IGMP Snooping L2-entry-limit: 65536
Global IGMPv2 Fast-Leave :Disable
Global multicast router learning mode :Enable
Query Max Respone Time: 10 (Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Dynamic Host Aging Time : 260(Seconds)

vlan 1
————————————

IGMP Snooping state: Enable
Multicast router learning mode: pim-dvmrp
IGMP Fast-Leave: Disable
IGMP VLAN querier: Disable
IGMP VLAN Mode: STATIC
```

【Prompt Information】-

【Platform Description】 -

11.24show ip multicast wlan

Show wireless multicast global switch.

show ip multicast wlan

【Parameter Description】

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to check whether the wireless multicast global switch is enabled.

【Configuration Example】1: Check whether the wireless multicast global switch is enabled

【Prompt Information】-

【Platform Description】 -

11.24show ip multicast wlan

Show wireless multicast global switch.

show ip multicast wlan

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to check whether the wireless multicast global switch is enabled.

【Configuration Example】1: Check whether the wireless multicast global switch is enabled.

```
AC-FS#show ip multicast wlan
Global multicast state:  enable
```

【Prompt Information】-

【Platform Description】 -

12 ACL

12.1 Command Identifier Table

The identifiers used in the following commands can be found in the following command identifier table:

Identifiers	Meaning
id	ACL numeric marker. Matchable range. IP Standard ACL: 1-99, 1300-1999. IP Extended ACLs: 100-199, 2000-2699 MAC Extended ACLs: 700-799. Expert Extended ACL: 2700-2899.
name	ACL Name.
sn	ACL table entry number (supports setting products by priority).
start-sn	Serial number starting value.
inc-sn	Serial number increment.
deny	If matched, access is denied.
permit	If matched, access is allowed.
port	For IPv6, the field can be ipv6, icmp, tcp, udp and the value 0-255, for IPv4, it can be one of eigrp, gre, ipinip, igmp, nos, ospf, icmp, udp, tcp, ip, or it can be the number 0-255 representing the IP protocol, some important protocols such as icmp/tcp/udp are listed separately Conduct Description.
interface idx	Enter the matching interface.
src	Message source address (host address or network address).
src-wildcard	Source address wildcard. Can be made non-contiguous, e.g. 0.255.0.32.
src-ipv6-pfix	Source IPv6 network address or network type.
dst-ipv6-pfix	Destination IPv6 network address or network type.
pfix-len	Number of bits from high mask.
src-ipv6-addr	Source IPv6 Address.
dst-ipv6-addr	Destination IPv6 address.
dscp	Differential service code point, code point value, range 0-63.
flow-label	Stream label, stream label value range 0-1048575.
dst	Message destination address (host address or network address).
dst-wildcard	Destination address wildcard. Can be discontinuous, e.g. 0.255.0.32.
Fragment	Filtering of message fragmentation. Description： None line does not support message fragmentation filtering.

precedence	Priority level of the message (0-7 in ascending order).
range	Layer 4 port number range for the message.
time-range tm-rng-name	Time zone for message filtering, with the name tm-rng-name.
tos	Service type of the message (0-15).
cos	The cos value of the message (0-7).
cos inner cos	The cos in the internal tag of the message.
icmp-type	Message type of the ICMP message (0-255).
icmp-code	Message type code of the ICMP message (0-255).
icmp-message	Message type name of the ICMP message.
operator port[port]	OOperator is the operator (lt-less than, eq-equal to, gt-greater than, neq-not equal to, range-range). port port number, two port numbers are needed for binomial operations, other operators just need a port number.
src-mac-addr	Physical address of the source host.
dst-mac-addr	Physical address of the destination host.
VID vid	Specified vlan id.
VID inner vid	Specify the vid in the internal tag.
ethernet-type	Ethernet protocol type, you can enter a 0x value.
match-all tcpf	Match all bits of the tcp flag.
established	Matches the rst or ack bit in the tcp flag flag, no other bits match.
text	Comment message.
in	Filter incoming messages to the interface.
out	Filter outgoing messages from this interface.
{rule mask offset}+	rule is the hexadecimal value field, mask is the hexadecimal mask field. offset is the offset, refer to the offset table. The "+" sign indicates at least one set of.
log	When a message matches an ACL rule, match log information is output.

The message fields are as follows:

AA AA AA AA AA AA BB BB BB BB BB BB CC CC DD DD DD DD EE FF GG HH HH HH II II JJ KK LL LL MM MM

NN NN OO PP QQ QQ RR RR RR RR SS SS SS SS TT TT

UU UU VV VV VV VV WW WW WW WW XY ZZ aa aa bb bb

The corresponding offset table is as follows:

Meaning	Offset	Alphabet	Meaning	Offset

Destination MAC	0	O	TTL Field	34
Source MAC	6	P	Protocol number	35
Data frame length Field	12	Q	IP Checksum	36
VLAN tag Field	14	R	Source ip address	38
DSAP (Destination Service Access Point) Field	18	S	Destination ip address	42
SSAP (Source Service Access Point) Field	19	T	TCP source port	46
Ctrl Field	20	U	TCP destination port	48
Org Code Field	21	V	Sequence number	50
Encapsulated data type	24	W	Confirmation Field	54
IP version number	26	XY	IP header length and reserved bits	58
TOS Field	27	Z	Reserved bits and flags bits	59
Length of IP packet	28	a	Windows size Field	60
ID number	30	b	Other	62
Flags Field	32			

The offset of each Field in the above table is their offset in the 802.3 data frame of SNAP+tag.

12.2 access-list

This command creates an ACL and adds an ACL rule to the ACL to filter data packets. The commands for creating different types of ACLs are as follows:

1. Create an IP standard ACL and add an ACL rule to the ACL

access-list id { deny | permit } { source source-wildcard | host source | any } [time-range tm-range-name] [log]

2. Create an IP extension ACL and add an ACL rule to the ACL

access-list id { deny | permit } protocol { source source-wildcard | host source | any } { destination destination-wildcard | host destination | any } [precedence precedence] [tos tos] [fragment] [range lower upper] [time -range time-range-name] [log]

3. Create a MAC extension ACL and add an ACL rule to the ACL

access-list id { deny | permit } { any | host source-mac-address } { any | host destination-mac-address} [ethernet-type] [cos [out] [inner in]]

4. Create an expert-level extended ACL and add an ACL rule to the ACL

access-list id { deny | permit } [protocol | [ethernet-type] [cos [out] [inner in]]] [VID [out] [inner in]]
{ source source-wildcard | host source | any } { host source-mac-address | any } { destination destination-wildcard | host destination | any }
{ host destination-mac-address | any }] [precedence precedence] [tos tos] [fragment] [range lower upper] [time-range time-range-name]

When selecting Field contains Ethernet type Ethernet-type or cos Field:
access-list id { deny | permit } { ethernet-type | cos [out] [inner in] } [VID [out] [inner in]] { source source-wildcard | host source | any }
{ host source-mac- address | any } { destination destination-wildcard | host destination | any } { host destination-mac-address | any }
[time-range time-range-name]

When the protocol Protocol Field is selected:
access-list id { deny | permit } protocol [VID [out] [inner in]] { source source-wildcard | host source | any } { host source-mac-address | any }
{ destination destination-wildcard | host destination | any } { host destination-mac-address | any } [precedence precedence] [tos tos]
[fragment] [range lower upper] [time-range time-range-name]

Expert extended ACLs for some important protocols:
Internet Control Message Protocol (ICMP):
access-list id { deny | permit } icmp [VID [out] [inner in]] { source source-wildcard | host source | any }
{ host source-mac-address | any } { destination destination-wildcard | host destination | any } { host destination-mac-address | any }
[icmp-type] [[icmp-type [icmp-code]] | [icmp -message]] [precedence precedence] [tos tos] [fragment] [time-range time-range-name]

Transmission Control Protocol (TCP):
access-list id { deny | permit } tcp [VID [out] [inner in]] { source source-wildcard | host Source | any }
{ host source-mac-address | any } [operator port [port]] { destination destination-wildcard | host destination | any } { host destination-mac-address | any } [operator port [port]] [precedence precedence] [tos tos] [fragment] [range lower upper] [time-range time-range-name] [match-all tcp-flag | established]

User Datagram Protocol (UDP):
access-list id { deny | permit } udp[VID [out] [inner in]] { source source –wildcard | host source | any }
{ host source-mac-address | any } [operator port [port]] { destination destination-wildcard | host destination | any } { host destination-mac-address | any } [operator port [port]] [precedence precedence] [tos tos] [fragment] [range lower upper] [time-range time-range-name]

Deletes the specified ACL.
no access-list id

【Parameter Description】

Parameter	Description
id	ACL number, assignable range: ● IP Standard ACLs (1-99, 1300-1999) ● IP Extended ACL (100-199, 2700 - 2899) ● MAC Extended ACL (700 - 799) ● Expert Extended ACL (2000 - 2699)
deny	If matched, access is denied.
permit	If matched, access is allowed.
source	Message source address (host address or network address).
source-wildcard	Source address wildcard. Can be non-contiguous, e.g. 0.255.0.32.
protocol	IP protocol number, which can be one of EIGRP, GRE, IPINIP, IGMP, NOS, OSPF, ICMP, UDP, TCP, IP ICMP, UDP, TCP, IP, or a number from 0-255 representing an IP protocol. A Some important protocols such as ICMP/TCP/UDP are listed separately for Description.
destination	Message destination address (host address or network address).
destination-wildcard	Destination address wildcard. Can be non-contiguous, e.g. 0.255.0.32.
destination-wildcard	Destination address wildcard. Can be non-contiguous, e.g. 0.255.0.32.
fragment	Filtering of message fragmentation.
precedence	Priority level of the message.
precedence	Priority level value of the message (0-7).
range	Layer 4 port number range for messages.
lower	Lower limit of the four-layer port number range.
upper	Upper limit of the four-layer port number range.
time-range	Time zone for message filtering.
time-range-name	Time zone name for message filtering.
tos	Service type of the message.
tos	Service type value of the message (0-15).
icmp-type	Message type of ICMP message (0-255).
icmp-code	Message type code of the ICMP message (0-255).
icmp-message	Message type name of the ICMP message.
operator	Operators (lt-less than, eq-equal to, gt-greater than, neq-not equal to,

	range-range).
port [port]	port number, range requires two port numbers, the other operators only need one port number.
host source-mac-address	The physical address of the source host.
host destination-mac-address	The physical address of the destination host.
VID vid	Match against the specified vid.
ethernet-type	Ethernet protocol type.
match-all	Match all bits of the tcp flag.
tcp-flag	tcp flag flag.
established	Matches rst or ack or bits in tcp flag and no other bits.
text	Note information.

【Default Configuration】 There is no ACL configuration and no ACL rule configuration

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 In order to use the access list to filter data, you must first define a series of access list rule statements through the command access-list. You can use different kinds of access lists depending on your specific needs:

1. IP standard ACLs (1-99, 1300-1999) control only source addresses.

2. IP extended ACL (100-199, 2000-2699), which can perform complex control based on source and destination addresses.

3. MAC Extended ACLs (700-799) that can be matched based on source and destination MAC addresses and Ethernet type.

4. Expert Extended Access Lists (2700-2899), a combination of IP Standard ACLs, IP Extended ACLs, and MAC Extended ACLs. It is allowed to configure the above three ACL rules in the expert-level extended ACL at the same time. In addition, the expert-level extended ACL can also perform matching filtering on VLAN IDs.

For Layer 3 routing protocols (including unicast routing protocols and multicast routing protocols), the following parameters in the access list rules are not supported: precedence precedence/tos tos/fragments/range lower upper/ time-range time-range-name.

TCP Flags contain some or all of the following:

urg

ack

psh

rst

syn

fin

The packet priority names are as follows:

critical

flash

flash-override

immediate

internet

network

priority

routine

The service type names are as follows:

max-reliability

max-throughput

min-delay

min-monetary-cost

normal

ICMP message type names are as follows:

administratively-prohibited

dod-host-prohibited

dod-net-prohibited

echo

echo-reply

fragment-time-exceeded

general-parameter-problem

host-isolated

host-precedence-unreachable

host-redirect

host-tos-redirect

host-tos-unreachable

host-unknown

host-unreachable

information-reply

information-request

mask-reply

mask-request

mobile-redirect

net-redirect

net-tos-redirect

net-tos-unreachable

net-unreachable

network-unknown

no-room-for-option

option-missing

packet-too-big

parameter-problem

port-unreachable

precedence-unreachable

protocol-unreachable

redirect

router-advertisement

router-solicitation

source-quench

source-route-failed

time-exceeded

timestamp-reply

timestamp-request

ttl-exceeded

unreachable

The following are the TCP port names, TCP can use the port name or port number to specify a specific port:

bgp

chargen

cmd

daytime

discard

domain

echo

exec

finger

ftp

ftp-data

gopher

hostname

ident

irc

klogin

kshell

login

nntp

pim-auto-rp

pop2

pop3

smtp

sunrpc

syslog

tacacs

talk

telnet

time

uucp

whois

www

The following are UDP port names, UDP can use port name or port number to specify a specific port:

biff

bootpc

bootps

discard

dnsix

domain

echo

isakmp

mobile-ip

nameserver

netbios-dgm

netbios-ns

netbios-ss

ntp

pim-auto-rp

rip

snmp

snmptrap

sunrpc

syslog

tacacs

talk

tftp

time

who

xdmcp

The Ethernet protocol type Ethernet-type is as follows:

aarp

arp

appletalk

decnet-iv

diagnostic

etype-6000

etype-8042

lat

lavc-sca

mop-console

mop-dump

mumps

netbios

vines-echo

xns-idp

If you want to delete an ACL rule, you need to enter the ACL mode and delete it with the no {sn | permit | deny} command.

【Configuration Example]】1: IP standard access list example

The following IP basic access list allows packets with source addresses 192.168.1.64 - 192.168.1.127 to pass, and all other packets are rejected:

```
AC-FS(config)# access-list 1 permit 192.168.1.64 0.0.0.63
```

2: IP Extended Access List Example

The following IP extension access list allows DNS packets and ICMP packets to pass through:

```
AC-FS(config)# access-list 102 permit tcp any any eq domain log
AC-FS(config)# access-list 102 permit udp any any eq domain log
AC-FS(config)# access-list 102 permit icmp any any echo log AC-
FS(config)# access-list 102 permit icmp any any echo-reply
```

3: Example of MAC Extended Access List

A source host with MAC 00d0f8000c0c is denied an Ethernet frame of type 100 and applied to interface gigabitethernet 1/1.

```
AC-FS(config)# access-list 702 deny host 00d0f8000c0c any aarp
AC-FS(config)# interface gigabitethernet 1/1
AC-FS(config-if-GigabitEthernet 1/1)# mac access-group 702 in
```

4: Expert Extended Access List Example

Create and display an Expert Extended ACL that denies a source IP address of 192.168.12.3 and a source MAC address of

All TCP packets of 00d0.f800.0044.

```
AC-FS(config)# access-list 2702 deny tcp host
192.168.12.3 mac 00d0.f800.0044 any any
AC-FS(config)# access-list 2702 permit any any any any AC-
FS(config)# show access-lists
expert access-list extended 2702
10 deny tcp  host  192.168.12.3 mac 00d0.f800.0044 any any
20 permit any any any any
```

【Verification】 1: Use the show access-lists command to view all ACL configuration information, including ACL rule information. 2: Use the show access-lists id command to view the configuration information of the specified ACL, including the ACL rule information. 3: Use the show access-lists name command to view the configuration information of the specified ACL, including the ACL rule information.

【Prompt Information】 If the same ACL rule is repeatedly added to the same ACL, an error message will be displayed:

failed, for the entry is existed or the sequence number has been allocated!

【Common Mistake】 -

【Platform Description】 -

12.3 access-list list-remark

Add comment information to the specified ACL.

access-list id list-remark text

Delete ACL comment information

no access-list id list-remark

【Parameter Description】

Parameter	Description
id	ACL number. Available ranges: IP Standard ACL (1-99, 1300-1999), IP Extended ACL (100-199, 2000-2699), MAC extended ACLs (700-799), expert extended ACLs (2700-2899).
text	Annotation Information.

【Default Configuration】 No ACL comment information.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 In order to check the function of a certain ACL, you can use this command to add comment information to the specified ACL. If the specified ACL does not exist, this command will create the ACL first, and then add comment information.

【Configuration Example]】1: Create an ACL numbered 1 and add the comment "this acl is to filter the host 192.168.4.12" to the ACL:

```
AC-FS(config)# ip access-list extended 100
AC-FS(config)# access-list 100 list-remark this acl is to filter the host 192.168.4.12
```

【Verification】1: Use the show access-lists command to view all ACL configuration information, including ACL comment information.

2: Use the show access-list sid command to view the configuration information of the specified ACL, including the comment information of the ACL.

3: Use the show access-lists name command to view the configuration information of the specified ACL, including the comment information of the ACL.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

12.4 access-list remark

Add comments for the ACL rules to be configured next.

access-list id remark text

Delete ACL rule comment information.

no access-list id remark text

【Parameter Description】

Parameter	Description
id	ACL number. Available ranges: IP Standard ACL (1-99, 1300-1999), IP Extended ACL (100-199, 2000-2699), MAC extended ACLs (700-799), expert extended ACLs （2700–2899）.
text	Note Information.

【Default Configuration】 No ACL rule comment information.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 In order to check the function of an ACL rule, you can use this command to add comment information to the specified ACL rule. If the specified ACL does not exist, this command will create the ACL first, and then add the ACL rule comment information

【Configuration Example]】1: Add an ACL rule comment to the ACL numbered 102:

```
AC-FS(config)# access-list 102 remark deny-host-10.1.1.1
```

【Verification】1: Use the show access-lists command to view all ACL configuration information, including the comment information of ACL rules.

2: Use the show access-lists id command to view the configuration information of the specified ACL, including the comment information of the ACL rule.

3: Use the show access-lists name command to view the configuration information of the specified ACL, including the comment information of the ACL rule.

【Prompt Information】 If the same ACL rule comment information is repeatedly added under the same ACL, an error message will be displayed:

Remark is duplicate.

【Common Mistake】 -

【Platform Description】 -

12.5deny

Add/remove a deny type ACL rule to an ACL.

1. IP Standard ACL

Add a deny type ACL rule to the IP standard ACL

[sn] deny { source source-wildcard | host source | any } [time-range tm-range-name] [log]

Remove a deny type ACL rule from the IP standard ACL

no { sn | { deny { source source-wildcard | host source | any } [time-range tm-range-name] [log] } }

2. IP Extended ACL

Add a deny type ACL rule to the IP extension ACL

[sn] deny protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [fragment] [range lower upper] [time-range time-range-name] [log]

Remove a deny type ACL rule from the IP extension ACL

no { sn | { deny protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [fragment] [range lower upper] [time-range time-range-name] [log] } }

IP Extended Access Control Lists for some important protocols:

Internet Control Message Protocol (ICMP)

[sn] deny icmp { source source-wildcard | host source | any } { destination destination-wildcard | host destination | any } [icmp-type] [[icmp-type [icmp-code]] | [icmp-message]] [precedence precedence] [tos tos] [fragment] [time-range time-range-name]

Transmission Control Protocol (TCP)

[sn] deny tcp { source source-wildcard | host Source | any } [operator port [port]] { destination destination-wildcard | host destination | any } [operator port [port]] [precedence precedence] [tos tos] [fragment] [range lower upper] [time-range time-range-name] [match-all tcp-flag | established]

User Datagram Protocol (UDP)

[sn] deny udp { source source –wildcard | host source | any } [operator port [port]] { destination destination-wildcard | host destination | any } [operator port [port]] [precedence precedence] [tos tos] [fragment] [range lower upper] [time-range time-range-name]

3. MAC Extended ACL

Add a deny type ACL rule to the MAC extended ACL

[sn] deny { any | host source-mac-address } { any | host destination-mac-address } [ethernet-type] [cos [out] [inner in]]

Remove a deny type ACL rule from the MAC extended ACL

no { sn | {deny { any | host source-mac-address } { any | host destination-mac-address} [ethernet-type] [cos [out] [inner in]] } }

4. Expert Extended ACL

Add a deny type ACL rule to the expert extended ACL

[sn] deny[protocol | [ethernet-type] [cos [out] [inner in]]] [[VID [out] [inner in]]] { source source-wildcard | host source | any}{host source- mac-address | any } { destination destination-wildcard |

host destination | any } { host destination-mac-address | any } [precedence precedence] [tos tos] [fragment] [range lower upper] [time-range time-range-name]

Remove a deny-type ACL rule from the expert extended ACL

no { sn | { deny [protocol | [ethernet-type] [cos [out] [inner in]]] [[VID [out] [inner in]]] { source source-wildcard | host source | any } { host source-mac-address | any } { destination destination-wildcard | host destination | any } { host destination-mac-address | any } [precedence precedence] [tos tos] [fragment] [range lower upper] [time-range time -range-name] } }

When selecting Field contains ethernet type ethernet-type or cos Field

[sn] deny { [ethernet-type } [cos [out] [inner in]] } [[VID [out] [inner in]]] { source source-wildcard | host source | any } { host source-mac- address | any } { destination destination-wildcard | host destination | any } { host destination-mac-address | any } [time-range time-range-name]

When selecting the protocol protocol Field

[sn] deny protocol [[VID [out] [inner in]]] { source source-wildcard | host source | any } { host source-mac-address | any } { destinationdestination-wildcard | host destination | any } { host destination-mac-address | any } [precedence precedence] [tos tos] [fragment] [range lower upper] [time-range time-range-name]

Expert extended access list for some important protocols:

Internet Control Message Protocol (ICMP)

[sn] deny icmp [[VID [out] [inner in]]] { source source-wildcard | host source | any } { host source-mac-address | any } { destination destination-wildcard | host destination | any } { host destination-mac-address | any } [icmp-type] [[icmp-type [icmp-code]] | [icmp-message]] [precedence precedence] [tos tos] [fragment] [time-range time-range -name]

Transmission Control Protocol (TCP)

[sn] deny tcp [[VID [out] [inner in]]] { source source-wildcard | host Source | any } { host source-mac-address | any } [operator port [port]] { destination destination-wildcard | host destination | any } { host destination-mac-address | any } [operator port [port]] [precedence precedence] [tos tos] [fragment] [range lower upper] [time-range time-range-name] [match-all tcp-flag | established]

User Datagram Protocol (UDP)

[sn] deny udp [[VID [out] [inner in]]] { source source –wildcard | host source | any } { host source-mac-address | any } [operator port [port]] { destination destination-wildcard | host destination | any } { host destination-mac-address | any } [operator port [port]] [precedence precedence] [tos tos] [fragment] [range lower upper] [time-range time-range-name]

Address Resolution Protocol (ARP)

[sn] deny arp { vid vlan-id } [source-mac-address source-wildcard | host source-mac-address | any] [host destination –mac-address | any] { sender-ip sender-ip –wildcard | host sender-ip | any } { sender-mac sender-mac-wildcard | host sender-mac | any } { target-ip target-ip–wildcard | host target-ip | any }

5. IPv6 Extended ACL

Add a deny type ACL rule to the IPv6 ACL

[sn] deny protocol { source-ipv6-prefix/prefix-length | any | host source-ipv6-address }

{ destination-ipv6-prefix / prefix-length | any | hostdestination-ipv6-address } [dscp dscp] [flow-label

flow-label] [fragment] [range lower upper] [time-range time-range-name]

Remove a deny-type ACL rule from the IPv6 ACL

no {sn | { deny protocol { source-ipv6-prefix/prefix-length | any | host source-ipv6-address }

{ destination-ipv6-prefix / prefix-length | any | hostdestination-ipv6-address } [dscp dscp] [flow-label

flow-label] [fragment] [range lower upper] [time-range time-range-name] } }

IPv6 extended access control lists for some important protocols:

Internet Control Message Protocol (ICMP)

[sn] deny icmp { source-ipv6-prefix / prefix-length | any source-ipv6-address | host }

{ destination-ipv6-prefix / prefix-length | host destination-ipv6-address | any } [icmp-type] [[icmp-type [icmp-code]] | [icmp-message]]

[dscp dscp] [flow- label flow-label] [fragment] [time-range time-range-name]

Transmission Control Protocol (TCP)

[sn] deny tcp { source-ipv6-prefix / prefix-length | hostsource-ipv6-address | any } [operator port [port]]

{ destination-ipv6-prefix /prefix-length | host destination-ipv6-address | any } [operator port [port]] [dscp dscp] [flow-label flow-label]

[fragment] [range lower upper] [time- range time-range-name] [match-all tcp-flag | established]

User Datagram Protocol (UDP)

[sn] deny udp { source-ipv6-prefix/prefix-length | host source-ipv6-address | any } [operator port [port]]

{ destination-ipv6-prefix /prefix-length | host destination-ipv6-address | any } [operator port [port]] [dscp

dscp] [flow-label flow-label] [fragment] [range lower upper] [time-range time-range-name]

【Parameter Description】

Parameter	Description
sn	ACL rule number.
source-ipv6-prefix	Source IPv6 network address or network type.
destination-ipv6-prefix	Destination IPv6 network address or network type.
prefix-length	high-order mask bits.
source-ipv6-address	source IPv6 address.
destination-ipv6-address	destination IPv6 address.
dscp	Poor service code point.
dscp	code point value, range 0-63.
flow-label	flow label.
flow-label	Stream label value, range 0-1048575.
protocol	For IPv6, this Field can be IPv6 | icmp | tcp | udp and <0-255>.
time-range	Time zone for packet filtering.
time-range-name	Time zone name for packet filtering.

【Default Configuration】 There is no ACL rule.

【Command Mode】 ACL mode

【Default Level】 14

【Usage Guide】 When you want to deny some packets from entering the network, you can use this command to add some deny-type ACL rules to the specified ACL.

【Configuration Example]】 1: The following example shows how to create and display an Expert Extended ACL that denies all TCP packets with source IP address 192.168.4.12 and source MAC address 001300498272.

```
AC-FS(config)# expert access-list extended 2702
AC-FS(config-exp-nacl)# deny tcp host
192.168.4.12 host 0013.0049.8272 any any AC-
FS(config-exp-nacl)# permit any any any any AC-
FS(config-exp-nacl)#  show  access-lists expert
access-list extended 2702
10 deny tcp  host  192.168.4.12 host 0013.0049.8272 any any
20 permit any any any any
AC-FS(config-exp-nacl)#
```

2: The following is an example of the use of IP extended ACL, the purpose is to deny the source host whose IP is 192.168.4.12 to provide services with TCP port 100, and apply it to the interface gigabitethernet 1/1. Configuration method:

```
AC-FS(config)# ip access-list extended ip-ext-acl AC-FS(config-
ext-nacl)# deny tcp host 192.168.4.12 eq 100 any AC-FS(config-
ext-nacl)# show access-lists
ip access-list extended ip-ext-acl
10 deny tcp host 192.168.4.12 eq 100 any
AC-FS(config-ext-nacl)# exit
AC-FS(config)# interface gigabitethernet 1/1
AC-FS(config-if-GigabitEthernet 0/1)# ip access-group ip-ext-acl in
```

3: The following is an example of the use of MAC extended ACL, the purpose is to deny the source host whose MAC is 0013.0049.8272 to send the Ethernet frame of type 100, and apply it to the interface gigabitethernet 1/1. Configuration method:

```
AC-FS(config)# mac access-list extended mac1 AC-FS(config-
mac-nacl)# deny host 0013.0049.8272 any aarp AC-FS(config-
mac-nacl)# show access-lists
mac access-list extended mac1
10 deny host 0013.0049.8272 any aarp AC-
FS(config-mac-nacl)#   exit AC-FS(config)#
interface gigabitethernet 1/1
AC-FS(config-if-GigabitEthernet 1/1)# mac access-group mac1 in
```

4: The following is an example of the use of IP standard ACL, the purpose is to deny the source host whose IP is 192.168.4.12, and apply it to the interface gigabitethernet1/1. Configuration method:

```
AC-FS(config)# ip access-list standard 34 AC-
FS(config-ext-nacl)# deny host 192.168.4.12 AC-
FS(config-ext-nacl)# show access-lists
ip  access-list  standard  34
10 deny host 192.168.4.12 AC-
FS(config-ext-nacl)# exit
AC-FS(config)# interface gigabitethernet 1/1
AC-FS(config-if-GigabitEthernet 1/1)# ip access-group 34 in
```

5: The following is an example of the use of IPv6 extended ACL, the purpose is to deny the source host whose IP is 192.168.4.12, and apply it to the interface gigabitethernet1/1. Configuration method:

```
AC-FS(config)# ipv6 access-list extended v6-acl AC-FS(config-
ipv6-nacl)# 11 deny ipv6 host 192.168.4.12 any AC-FS(config-
ipv6-nacl)# show access-lists
ipv6 access-list  extended  v6-acl
11 deny ipv6 host 192.168.4.12 any
AC-FS(config-ipv6-nacl)# exit
AC-FS(config)# interface gigabitethernet 1/1
AC-FS(config-if-GigabitEthernet 1/1)# ipv6 traffic-filter v6-acl in
```

【Verification】 1: Use the show access-lists command to view the configuration information of all ACLs, including all the rules configured under the ACL. 2: Use the show access-lists id command to view the configuration information of the specified ACL, including all the rules configured under the ACL. 3: Use the show access-lists name command to view the configuration information of the specified ACL, including all the rules configured under the ACL.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

12.6 clear counters access-list

Clears the statistics of packet matching in the ACL.

clear counters access-list [id | name]

【Parameter Description】

Parameter	Description
id	ACL number. Configurable range: IP standard ACL (1-991300-1999), IP extension ACL (100-1992000-2699), MAC extension ACL (700–799), expert extension Exhibition ACL (2700–2899).
name	Names of ACLs.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 If you want to restart the statistics of the packet matching information of the specified ACL, you can execute this command to clear the packet matching statistics value of the ACL to zero.

【Configuration Example]】 1: Clear the count value of the packet matching statistics of the ACL numbered 2700 to zero. Before using this command:

```
AC-FS #show access-lists 2700
expert access-list extended 2700
    10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any  (88 matches)
    20 deny tcp any any eq login any any (33455 matches)
    30 permit tcp any any host 192.168.6.9 any (10 matches)
```

After using this command:

```
AC-FS# clear counters access-list 2700
AC-FS #show access-lists 2700
expert access-list extended 2700
    10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any
    20 deny tcp any any eq login any any
    30 permit tcp any any host 192.168.6.9 any
```

【Prompt Information】-

【Platform Description】 -

12.7 clear access-list counters

Clears the statistics of ACL deny packets.

clear access-list counters [id | name]

【Parameter Description】

Parameter	Description
id	ACL numbering. Available ranges: IP Standard ACL (1-99, 1300-1999), IP Extended ACL (100-199, 2000-2699), MAC Extended ACL (700-799), Expert Extended ACL (2700-2899).
name	Names of ACLs.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 If you want to restart the statistics of the packet matching information of the specified ACL that is denied, you can execute this command to clear the matching statistics value of the denied packets of the ACL to zero.

【Configuration Example]】1: Clear the count value of the packet matching statistics of the ACL numbered 1 to zero. Before using this command:

```
AC-FS #show access-lists
ip access-list standard 1
    10 deny host 50.1.1.2 (10 matches)
    20 permit host 60.1.1.2 (15 matches)
    (10 packets filtered)
```

After using this command:

```
AC-FS# end
AC-FS# clear access-list counters AC-FS#
show access-lists
ip access-list standard 1
    10 deny host 50.1.1.2 (10 matches)
    20 permit host 60.1.1.2 (15 matches)
```

【Prompt Information】-

【Platform Description】 -

12.8expert access-group

Applies a specified expert-level ACL to the inbound or outbound direction of the specified interface.

expert access-group { id | name } { in | out }

Cancel the application of expert-level ACL in the inbound or outbound direction on the specified interface

no expert access-group { id | name } { in | out }

【Parameter Description】

Parameter	Description
id	Numbering of Expert ACLs (2700-2899).
name	The name of the expert ACL.
in	Filtering of incoming messages to this interface.
out	Filtering of outgoing messages from this interface.

【Default Configuration】 Expert ACL is not applied to the interface.

【Command Mode】 Interface mode

【Default Level】 14

【Usage Guide】 To make the expert-level ACL take effect, you need to apply the ACL to the specified interface, then you can use this command in the interface configuration mode.

【Configuration Example]】1: Apply an expert-level ACL named accept_00d0f8xxxxxx_only to GigaEthernet 0/1:

```
AC-FS(config)# interface GigaEthernet 0/1
AC-FS(config-if-GigabitEthernet 0/1)# expert access-group accept_00d0f8xxxxxx_only in
```

【Verification】1: Use the show expert access-group command to view the expert-level ACLs applied on all interfaces.

2: Use the show expert access-group interface interface-name command to view the expert-level ACL applied to the specified interface.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

12.9expert access-list extended

Create an expert extended ACL and enter this configuration mode.

expert access-list extended { id | name }

Delete Expert Extended ACL

no expert access-list extended { id | name }

【Parameter Description】

Parameter	Description
id	Numbering of expert extension ACLs (2700-2899)
name	Name of the expert extension ACL

【Default Configuration】 Expert-level extended ACL is not created.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 If you want to achieve the filtering effect of IP standard ACL, IP extended ACL and MAC extended ACL in one ACL, you can use expert extended ACL.

【Configuration Example]】1: Create an expert-level extended ACL named "exp-acl":

```
AC-FS(config)# expert access-list extended exp-acl
AC-FS(config-exp-nacl)# show access-lists
expert access-list extended exp-acl
AC-FS(config-exp-nacl)#
```

2: Create an expert extended ACL numbered 2704:

```
AC-FS(config)# expert access-list extended 2704
AC-FS(config-exp-nacl)#  show  access-lists
expert access-list extended 2704
AC-FS(config-exp-nacl)#
```

【Verification】 1: Use the show access-lists command to view all configured ACL information, including expert ACLs.

2: Use the show access-lists id command to view the ACL information of the specified number, including the expert ACL.

3: Use the show access-lists name command to view the ACL information of the specified name, including the expert ACL.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

12.10expert access-list sequence

Reorder the sequence numbers of the rule entries of the expert-level extended ACL.

expert access-list resequence { id | name } start-sn inc-sn

Restore defaults.

no expert access-list resequence { id | name }

【Parameter Description】

Parameter	Description
id	Numbering of Expert Extension ACLs (2700-2899).
name	The name of the expert extended ACL.
start-sn	Serial number starting value (1-2147483647).
inc-sn	Serial number increment (1-2147483647).

【Default Configuration】 start-sn: 10

inc-sn: 10

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 In actual use, it is possible to perform multiple operations of adding and deleting rules in the expert-level extended ACL. After a period of time, the serial number will become messy. At this time, you can use this command to modify the ACL rules. The sequence numbers of table entries are rearranged to make the sequence numbers regular.

【Configuration Example]】 1: Rearrange the expert-level extended ACL rule entries named "exp-acl" according to the starting sequence number of 21 and the increment of 43. Before configuring this command:

```
AC-FS# show access-lists
expert access-list extended exp-acl
 10 permit ip any any any any
 20 deny ip any any any any
```

After configuring this command:

```
AC-FS# config
AC-FS(config)# expert access-list resequence exp-acl 21 43 AC-
FS(config)# exit
AC-FS# show access-lists
expert access-list extended exp-acl
 21 permit ip any any any any
 64 deny ip any any any any
```

【Verification】 1: Use the show access-lists command to view the latest sequence numbers of rule entries under all ACLs. 2: Use the show access-lists id command to view the latest sequence number of the rule entry under the specified ACL. 3: Use the show access-lists name command to view the latest sequence number of the rule entry under the specified ACL.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

12.11ip access-group

Apply the specified ACL to the interface

ip access-group { id | name } { in | out }

Disassociate an ACL from an interface

no ip access-group { id | name } { in | out }

【Parameter Description】

Parameter	Description
id	Number of IP Standard ACL or IP Extended ACL (1-199, 1300-2699).
name	The name of the IP standard ACL or IP extended ACL.
in	Filtering of incoming messages to this interface.
out	Filtering of outgoing messages from this interface.

【Default Configuration】 No ACL is applied to the interface.

【Command Mode】 Interface mode

【Default Level】 14

【Usage Guide】 To make the IP standard ACL or IP extended ACL take effect, you can use this command to apply the ACL to an interface, so that the incoming and outgoing packets on the interface can be controlled.

【Configuration Example]】1: Apply ACL number 120 on fastEthernet0/0 to filter incoming packets:

```
AC-FS(config)# interface fastEthernet 0/0
AC-FS(config-if-GigabitEthernet 0/0)#ip access-group 120 in
```

【Verification】1: Use the show ip access-group command to view the application information of all IP standard and IP extended ACLs

2: Use the show ip access-group interface interface-name command to view the IP standard and IP extension on the specified interface Application information of the ACL.

【Prompt Information】1: When applying an ACL on an interface, if an ACL of the following types is already applied in the same direction of the interface, an error message will be displayed: IP standard ACL, IP extended ACL, MAC extended ACL, and expert ACL.

Another acl has attached at GigabitEthernet 0/2, Operation fail.

2: When canceling the application of the ACL on the interface, if the specified ACL is not applied to the specified direction of the interface, an error message will be displayed:

The acl has not attached at %s, Operation fail

【Common Mistake】-

【Platform Description】 -

12.12ip access-list

Create an IP Standard ACL or IP Extended ACL and enter ACL mode.

ip access-list { extended | standard } { id | name }

Delete this ACL.

no ip access-list { extended | standard } { id | name }

【Parameter Description】

Parameter	Description
id	IP access list numbering, standard (1-99, 1300-1999), extended (100-199, 2000-2699).
name	Name of the IP access list.

【Default Configuration】No ACL.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 If you only want to match and filter IP packets based on source IP, you can create an IP standard ACL; if you want to control IP packets more finely, for example, you want to filter packets based on destination IP or even based on Layer 4 information. To match and filter the text, you need to create an IP extended ACL. For the fields that can be matched by two IP ACLs, please refer to the standard and extended forms of deny and permit commands. Use the show access-lists command to view ACL settings.

【Configuration Example]】1: Create a standard IP ACL named "std-acl":

```
AC-FS(config)# ip access-list standard std-acl
AC-FS(config-std-nacl)# show access-lists
ip access-list standard std-acl
AC-FS(config-std-nacl)#
```

2: Create an extended ACL numbered "123":

```
AC-FS(config)# ip access-list extended 123
AC-FS(config-ext-nacl)# show access-lists
ip access-list extended 123
```

【Verification】Use the show access-lists command to view the ACL configuration.

【Prompt Information】 1: When creating a named IP standard or IP extended ACL, if the specified name has been used by other types of ACLs, an error message will be displayed:

```
ACL type error, current ACL has been set to type %s. (where %s is one of ip standard, ip extended, mac extended, expert extended, expert advanced, and ipv6).
```

2: When creating a named IP standard or IP extended ACL, if the number of named ACLs (all types of named ACLs) created in the device has reached 500, an error message will be displayed:

```
Failed to create user-defined acl for the max-limit has been reached
```

3: When creating a named IP standard or IP extended ACL, if the input name is longer than 99 characters, an error message will be displayed:

```
Name is too long
```

4: When creating a named IP standard or IP extended ACL, if the input name starts with a number, or the name is "in" or "out", an error message will be displayed:

```
Invalid name
```

【Common Mistake】-

【Platform Description】 -

12.13ip access-list sequence

Reorder the sequence number of the rule table entry of IP standard ACL or IP extended ACL

ip access-list resequence { id | name } start-sn inc-sn

Restore Defaults

no ip access-list resequence { id | name }

【Parameter Description】

Parameter	Description
id	IP Standard ACL or IP Extended ACL numbering, Standard (1-99, 1300-1999), Extended (100-199, 2000-2699.)
name	ACL Name for IP Standard ACL or IP Extended ACL.

start-sn	Serial number starting value (1-2147483647).
inc-sn	Serial number increment (1-2147483647).

【Default Configuration】 start-sn: 10

inc-sn: 10

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 In actual use, it is possible to perform multiple operations of adding and deleting rules in IP standard ACL or IP extended ACL. After a period of time, the serial number will become messy. In this case, you can use this command Rearrange the sequence numbers of ACL rule entries to make the sequence numbers regular.

【Configuration Example】】 1: Rearrange the ACL rule entry numbered 1 according to the starting sequence number of 21 and the increment of 43. Before configuring this command:

```
AC-FS#  show  access-lists
ip access-list  standard  1
10 permit host 192.168.4.12
20 deny any any
```

After configuring this command:

```
AC-FS# config
AC-FS(config)# ip access-list resequence 1 21 43
AC-FS(config)# exit
AC-FS#  show  access-lists
ip access-list  standard  1
21 permit host 192.168.4.12
64 deny any any
```

【Verification】 1: Use the show access-lists command to view the latest sequence numbers of rule entries under all ACLs. 2: Use the show access-lists id command to view the latest sequence number of the rule entry under the specified ACL. 3: Use the show access-lists name command to view the latest sequence number of the rule entry under the specified ACL.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

12.14ipv6 access-list

Create an IPv6 ACL and enter this configuration mode.

ipv6 access-list name

delete this ACL.

no ipv6 access-list name

【Parameter Description】

Parameter	Description
name	IPv6 ACL Name

【Default Configuration】 No IPv6 ACL.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 If you want to perform security filtering on IPv6 packets in the network, you need to use IPv6 ACL. First, use this command to create an IPv6 ACL.

【Configuration Example]】1: Create an IPv6 ACL named "v6-acl":

```
AC-FS(config)# ipv6 access-list v6-acl AC-
FS(config-ipv6-nacl)# show access-lists ipv6
access-list v6-acl
AC-FS(config-ipv6-nacl)#
```

【Verification】1: Use the show access-lists command to view the configuration information of all ACLs (including IPv6 ACLs). 2: Use the show access-lists name command to see the configuration information of the specified ACL (including IPv6 ACL).

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

12.15ipv6 access-list sequence

Rearrange the sequence number of the rule table entry of the IPV6 ACL.

ipv6 access-list resequence name start-sn inc-sn

Restore Defaults.

no ipv6 access-list resequence name

【Parameter Description】

Parameter	Description
name	IPv6 ACL Name.
start-sn	Serial number start value (1-2147483647).
inc-sn	Serial number increment (1-2147483647).

【Default Configuration】 start-sn: 10

inc-sn: 10

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 In actual use, it is possible to perform multiple operations of adding and deleting rules in IPV6 ACL. After a period of time, the serial number will become messy. The sequence numbers are rearranged to make the sequence numbers regular.

【Configuration Example]】 1: Rearrange the IPv6 ACL rule entries named "v6-acl" according to the starting sequence number of 21 and the increment of 43. Before configuring this command:

```
AC-FS# show access-lists
ipv6 access-list v6-acl
 10 permit ipv6 any any
 20 deny ipv6 any any
```

After configuring this command:

```
AC-FS# config
AC-FS(config)# ipv6 access-list resequence v6-acl 21 43 AC-
FS(config)# exit
AC-FS# show access-lists
ipv6 access-list v6-acl
 21 permit ipv6 any any
 64 deny ipv6 any any
```

【Verification】 1: Use the show access-lists command to view the latest sequence numbers of rule entries under all ACLs.

2: Use the show access-lists name command to view the latest sequence number of the rule entry under the specified ACL.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

12.16 ipv6 traffic-filter

Apply an IPv6 ACL to the specified interface.

ipv6 traffic-filter name { in | out }

Cancel IPv6 ACL application.

no ipv6 traffic-filter name { in | out }

【Parameter Description】

Parameter	Description
name	Name of the IPv6 ACL.
in	Filtering of incoming messages to this interface.
out	Filtering of outgoing messages from this interface.

【Default Configuration】 No IPv6 ACL is applied to the interface.

【Command Mode】 Interface mode

【Default Level】 14

【Usage Guide】 To make the IPv6 ACL take effect, you can use this command to apply the ACL to an interface, so that the incoming and outgoing IPv6 packets on the interface can be controlled.

【Configuration Example]】1: Apply access-list v6-acl to Gigabit interface 0/1:

```
AC-FS(config)# interface GigaEthernet 0/1
AC-FS(config-if-GigabitEthernet 0/1)# ipv6 traffic-filter v6-acl in
```

【Verification】1: Use the show ipv6 traffic-filter command to view the application configuration of all IPv6 ACLs.

2: Use the show ipv6 traffic-filter interface interface-name command to view the IPv6 ACL application configuration on the specified interface.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

12.17list-remark

Add comment information to the specified ACL

list-remark text

Delete ACL comment information

no list-remark

【Parameter Description】

Parameter	Description
text	Note Information,

【Default Configuration】 No ACL comment information.

【Command Mode】ACL mode

【Default Level】 14

【Usage Guide】 In order to check the function of a certain ACL, you can use this command to add comment information to the specified ACL. You can also use the access-list list-remark command in global configuration mode to add comment information to an ACL.

【Configuration Example】】 1: Add the comment information of "this acl is to filter the host 192.168.4.12" to the IP extension ACL numbered 102:

```
AC-FS(config)# ip access-list extended 102
AC-FS(config-ext-nacl)# list-remark this acl is to filter the host 192.168.4.12
AC-FS(config-ext-nacl)# show access-lists
ip access-list extended 102
deny ip host 192.168.4.12 any
1000 hits
this acl is to filter the host 192.168.4.12
AC-FS(config-ext-nacl)#
```

【Verification】1: Use the show access-lists command to view all ACL configuration information, including ACL comment information.

2: Use the show access-lists id command to view the configuration information of the specified ACL, including the comment information of the ACL.

3: Use the show access-lists name command to view the configuration information of the specified ACL, including the comment information of the ACL.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

12.18mac access-group

Applies a MAC extended ACL to the specified interface.

mac access-group { id | name } { in | out }

Cancel MAC Extended ACL Application

no mac access-group { id | name } { in | out }

【Parameter Description】

Parameter	Description
id	Number of MAC Extended ACL (700-799).
name	The name of the MAC extended ACL.

in	Filtering of incoming packets to this interface.
out	Filtering of outgoing packets from this interface.

【Default Configuration】 No MAC extended ACL is applied to the interface.

【Command Mode】 Interface mode

【Default Level】 14

【Usage Guide】 To make the MAC extended ACL take effect, you can use this command to apply the ACL to an interface, so that the incoming and outgoing Ethernet packets on the interface can be controlled.

【Configuration Example]】 1: Apply the MAC extended ACL named "accept_00d0f8xxxxxx_only" to interface GigaEthernet 1/1:

```
AC-FS(config)# interface GigaEthernet 1/1
AC-FS(config-if-GigabitEthernet 1/1)# mac access-group accept_00d0f8xxxxxx_only in
```

【Verification】 1: Use the show mac access-group command to view the application information of all MAC extended ACLs.
2: Use the show mac access-group interface interface-name command to view the application information of the MAC extended ACL on the specified interface.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

12.19mac access-list extended

Create a MAC extended ACL and enter ACL mode

mac access-list extended { id | name }

Delete MAC Extended ACL

no mac access-list extended { id | name }

【Parameter Description】

Parameter	Description
id	Number of MAC Extended ACL (700-799).
name	The name of the MAC extended ACL.

【Default Configuration】 There is no MAC extended ACL.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 If you want to perform security filtering on Layer 2 packets in the network, you need to use a MAC extended ACL. First, you need to use this command to create a MAC extended ACL.

【Configuration Example]】1: Create a MAC extended ACL named "mac-acl":

```
AC-FS(config)# mac access-list extended mac-acl
AC-FS(config-mac-nacl)# show access-lists
mac access-list extended mac-acl
```

2: Create a MAC extended ACL numbered 704:

```
AC-FS(config)# mac access-list extended 704
AC-FS(config-mac-nacl)# show access-lists
mac access-list extended 704
```

【Verification】1: Use the show access-lists command to view the configuration information of all ACLs.

2: Use the show access-lists id command to view the configuration information of the specified ACL. 3: Use the show access-lists name command to view the configuration information of the specified ACL.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

12.20mac access-list sequence

Reorder the sequence numbers of the rule entries of the MAC extended ACL

mac access-list resequence { id | name } start-sn inc-sn

Restore Defaults

no mac access-list resequence { id | name }

【Parameter Description】

Parameter	Description
id	Number of MAC Extended ACL (700-799).
name	Name of the MAC extended ACL.
start-sn	Serial number starting value (1-2147483647).
inc-sn	Serial number increment (1-2147483647).

【Default Configuration】 start-sn: 10

inc-sn: 10

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 In actual use, it is possible to perform multiple operations of adding and deleting rules in the MAC extended ACL. After a period of time, the serial number will become messy. At this time, you can use this command to modify the ACL rule table. The sequence number of the item is rearranged to make the sequence number regular.

【Configuration Example]】1: Rearrange the MAC extended ACL rule entries named "mac-acl" according to the starting sequence number of 21 and the increment of 43. Before configuring this command:

AC-FS# show access-lists

```
mac access-list extended mac-acl
 10 permit any any etype-any
 20 deny any any etype-any
```

After configuring this command:

```
AC-FS# config
AC-FS(config)# mac access-list resequence exp-acl 21 43 AC-
FS(config)# exit
AC-FS# show access-lists
mac access-list extended mac-acl
 21 permit any any etype-any
 64 deny any any etype-any
```

【Verification】 1: Use the show access-lists command to view the latest sequence numbers of rule entries under all ACLs.

2: Use the show access-lists id command to view the latest sequence number of the rule entry under the specified ACL. 3: Use the show access-lists name command to view the latest sequence number of the rule entry under the specified ACL.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

12.21permit

Add/remove an allow-type ACL rule to an ACL.

6. IP Standard ACL

Add an allow-type ACL rule to the IP Standard ACL

[sn] permit { source source-wildcard | host source | any } [time-range tm-range-name] [log]

Remove an ACL rule of the allow type from the IP Standard ACL

no { sn | { permit { source source-wildcard | host source | any } [time-range tm-range-name] [log] } }

7. IP Extended ACL

Add an allow type ACL rule to the IP extension ACL

[sn] permit protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [fragment] [range lower upper] [time-range time-range-name] [log]

Remove an ACL rule of the allow type from the IP extension ACL

no { sn | { permit protocol source source-wildcard destination destination-wildcard [precedence

precedence] [tos tos] [fragment] [range lower upper] [time-range time-range-name] [log] } }

IP Extended Access Control Lists for some important protocols:

Internet Control Message Protocol (ICMP):

[sn] permit icmp { source source-wildcard | host source | any } { destination destination-wildcard | host destination | any } [icmp-type]

[[icmp-type [icmp-code]] | [icmp-message]] [precedence precedence] [tos tos] [fragment] [time-range time-range-name]

Transmission Control Protocol (TCP):

[sn] permit tcp { source source-wildcard | host Source | any } [operator port [port]] { destination destination-wildcard | host destination |

any } [operator port [port]] [precedence precedence] [tos tos] [fragment] [range lower upper] [time-range time-range-name]

[match-all tcp-flag | established]

User Datagram Protocol (UDP):

[sn] permit udp { source source –wildcard | host source | any } [operator port [port]] { destination destination-wildcard | host destination

| any } [operator port [port]] [precedence precedence] [tos tos] [fragment] [range lower upper] [time-range time-range-name]

8. MAC Extended ACL

Add an allow-type ACL rule to the MAC extended ACL

[sn] permit { any | host source-mac-address } { any | host destination-mac-address } [ethernet-type] [cos

[out] [inner in]]

Remove an ACL rule of the allow type from the MAC extended ACL

no { sn | { permit { any | host source-mac-address } { any | host destination-mac-address } [ethernet-type] [cos [out] [inner in]] } }

9. Expert Extended ACL

Add an allow-type ACL rule to the Expert Extended ACL

[sn] permit [protocol | [ethernet-type] [cos [out] [inner in]]] [VID [out] [inner in]] { source source-wildcard | host source | any }

{ host source-mac- address | any } { destination destination-wildcard

| host destination | any } { host destination-mac-address | any } [precedence precedence] [tos tos] [fragment] [range lower upper]

[time-range time-range-name]

Remove an ACL rule of the allow type from the Expert Extended ACL

no { sn | { permit [protocol | [ethernet-type] [cos [out] [inner in]]] [VID [out] [inner in]] { source

source-wildcard | host source | any } { host source-mac-address | any } { destination destination-wildcard

| host destination | any } { host destination-mac-address | any } [precedence precedence] [tos tos] [fragment] [range lower upper]

[time-range time-range-name] } }

When selecting Field contains Ethernet type Ethernet-type or cos Field:

[sn] permit { ethernet-type | cos [out] [inner in] } [VID [out] [inner in]] { source source-wildcard | host source | any } { host source-mac-address | any } { destination destination-wildcard | host destination | any } { host destination-mac-address | any } [time-range time-range-name]

When the protocol Protocol Field is selected:

[sn] permit protocol [VID [out] [inner in] { source source-wildcard | host Source | any } { host source-mac-address | any } { destination destination-wildcard | host destination | any } { host destination- mac-address | any } [precedence precedence] [tos tos] [fragment] [range lower upper] [time-range time-range-name]

Internet Control Message Protocol (ICMP):

[sn] permit icmp [VID [out] [inner in]] { source source-wildcard | host source | any } { host source-mac-address | any } { destination destination-wildcard | host destination | any } { host destination -mac-address | any } [icmp-type] [[icmp-type [icmp-code]] | [icmp-message]] [precedence precedence] [tos tos] [fragment] [time-range time-range-name]

Transmission Control Protocol (TCP):

[sn] permit tcp [VID [out] [inner in]] { source source-wildcard | host Source | any } { host source-mac-address | any } [operator port [port]] { destination destination-wildcard | host destination | any } { host destination-mac-address | any } [operator port [port]] [precedence precedence] [tos tos] [fragment] [range lower upper] [time-range time-range-name] [match- all tcp-flag | established]

User Datagram Protocol (UDP)

[sn] permit udp [VID [out] [inner in]] { source source –wildcard | host source | any } { host source-mac-address | any } [operator port [port]] { destination destination-wildcard | host destination | any } { host destination-mac-address | any } [operator port [port]] [precedence precedence] [tos tos] [fragment] [range lower upper] [time-range time-range-name]

Address Resolution Protocol (ARP)

[sn] permit arp { vid vlan-id } [host source-mac-address | any] [host destination –mac-address | any]

{ sender-ip sender-ip–wildcard | host sender-ip | any } { sender-mac sender-mac-wildcard | host sender-mac

| any } { target-ip target-ip–wildcard | host target-ip | any }

10. Expert Advanced ACL

Add an allow-type ACL rule to the Expert Advanced ACL

[sn] permit hex hex-mask offset

Remove an ACL rule of the allow type from the Expert Advanced ACL

no { sn | permit hex hex-mask offset }

11. IPv6 Extended ACL

Add an allow-type ACL rule to the IPv6 ACL

[sn] permit protocol { source-ipv6-prefix / prefix-length | any | host source-ipv6-address}

{ destination-ipv6-prefix / prefix-length | any | hostdestination-ipv6-address } [dscp dscp] [flow-label

flow-label] [fragment] [range lower upper] [time-range time-range-name]

Remove an allow-type ACL rule from the IPv6 ACL

no { sn | { permit protocol { source-ipv6-prefix / prefix-length | any | host source-ipv6-address}

{ destination-ipv6-prefix / prefix-length | any| hostdestination-ipv6-address } [dscp dscp] [flow-label

flow-label] [fragment] [range lower upper] [time-range time-range-name] } }

Internet Control Message Protocol (ICMP)

[sn] permit icmp { source-ipv6-prefix / prefix-length | any source-ipv6-address | host}

{ destination-ipv6-prefix / prefix-length | host destination-ipv6-address | any } [icmp-type] [[icmp-type [icmp-code]] | [icmp-message]]

[dscp dscp] [flow- label flow-label] [fragment] [time-range time-range-name]

Transmission Control Protocol (TCP)

[sn] permit tcp { source-ipv6-prefix / prefix-length | host source-ipv6-address | any } [operator port [port]]

{ destination-ipv6-prefix / prefix-length | host destination-ipv6-address | any } [operator port [port]] [dscp dscp] [flow-label flow-label]

[fragment] [range lower upper] [time- range time-range-name] [match-all tcp-flag | established]

User Datagram Protocol (UDP)

[sn] permit udp { source-ipv6-prefix / prefix-length | host source-ipv6-address | any } [operator port [port]] { destination-ipv6-prefix /

prefix-length | host destination-ipv6-address | any } [operator port [port]] [dscp dscp] [flow-label flow-label] [fragment] [range lower

upper] [time-range time-range-name]

【Parameter Description】

Parameter	Description

sn	ACL rule number.
source-ipv6-prefix	Source IPv6 network address or network type.
destination-ipv6-prefix	Destination IPv6 network address or network type.
prefix-length	Number of bits from high mask.
source-ipv6-address	Source IPv6 address.
destination-ipv6-address	Destination IPv6 address.
dscp	Differential Service Code Points.
dscp	Code point value, range 0-63.
flow-label	Stream Label.
flow-label	Stream tag value, in the range 0-1048575.
protocol	For IPv6, this Field can be IPv6 | icmp | tcp | udp and <0-255>.
time-range	Time zone for message filtering.
time-range-name	Time zone name for message filtering.
hex	Matching field in hexadecimal notation, used when configuring expert-level advanced ACL rules.
hex-mask	Matching domain mask in hexadecimal, used when configuring expert-level advanced ACL rules.
offset	Match start location, used when configuring expert-level advanced ACL rules.

【Default Configuration】 No ACL rule configuration.

【Command Mode】ACL mode

【Default Level】 14

【Usage Guide】 When you want to allow certain packets to enter the network, you can use this command to add some allow-type ACL rules to the specified ACL.

【Configuration Example]】1: The following example shows how to create and display an Expert Extended ACL that allows all TCP packets with source IP address 192.168.4.12 and source MAC address 001300498272.

```
AC-FS(config)# expert access-list extended exp-acl
AC-FS(config-exp-nacl)# permit tcp host 192.168.4.12 host 0013.0049.8272 any any AC-
FS(config-exp-nacl)# deny any any any any
AC-FS(config-exp-nacl)# show access-lists
expert access-list extended exp-acl
10 permit tcp  host  192.168.4.12 host 0013.0049.8272 any any
20 deny any any any any
AC-FS(config-exp-nacl)#
```

2: The following is an example of the use of IP extended ACL, the purpose is to allow the source host whose IP is 192.168.4.12 to provide services with TCP port 100, and apply it to the interface gigabitethernet 1/1. Configuration method:

```
AC-FS(config)# ip access-list extended 102
AC-FS(config-ext-nacl)# permit tcp host 192.168.4.12 eq 100 any
AC-FS(config-ext-nacl)# show access-lists
ip access-list extended 102
10 permit tcp host 192.168.4.12 eq 100 any
AC-FS(config-ext-nacl)# exit
AC-FS(config)# interface gigabitethernet 1/1
AC-FS(config-if-GigabitEthernet 1/1)# ip access-group 102 in
```

3: The following is an example of the use of MAC extended ACL, the purpose is to allow the source host with MAC 0013.0049.8272 to send Ethernet frames of type 100 and apply to the interface gigabitethernet 1/1. Configuration method:

```
AC-FS(config)# mac access-list extended 702
AC-FS(config-mac-nacl)# permit host 0013.0049.8272 any aarp
AC-FS(config-mac-nacl)# show access-lists
mac access-list extended
10 permit host 0013.0049.8272 any aarp702
AC-FS(config-mac-nacl)# exit
AC-FS(config)# interface gigabitethernet 1/1
AC-FS(config-if-GigabitEthernet 1/1)# mac access-group 702 in
```

4: The following is an example of ip standard ACL usage, the purpose is to allow the source host whose IP is 192.168.4.12, and apply it to interface 1. Configuration method:

```
AC-FS(config)# ip access-list standard std-acl AC-
FS(config-std-nacl)# permit host 192.168.4.12 AC-
FS(config-std-nacl)# show access-lists
ip access-list standard std-acl
10 permit host 192.168.4.12 AC-
FS(config-std-nacl)# exit
AC-FS(config)# interface gigabitethernet 1/1
AC-FS(config-if-GigabitEthernet 1/1)# ip access-group std-acl in
```

5: The following is an example of IPv6 extended ACL usage, the purpose is to allow the source host whose IP is 192.168.4.12, and apply it to interface gigabitethernet1/1. Configuration method:

```
AC-FS(config)# ipv6 access-list extended v6-acl
AC-FS(config-ipv6-nacl)# 11 permit ipv6 host ::192.168.4.12 any
AC-FS(config-ipv6-nacl)# show access-lists
ipv6 access-list extended v6-acl
11 permit ipv6 host ::192.168.4.12 any AC-
FS(config-ipv6-nacl)#  exit AC-FS(config)#
interface gigabitethernet 1/1
AC-FS(config-if-GigabitEthernet 1/1)# ipv6 traffic-filter v6-acl in
```

6: The following is an example of expert-level advanced ACL usage, the purpose is to allow the source host whose IP is 192.168.4.12, and apply it to the interface gigabitethernet 1/1. Configuration method:

```
AC-FS(config)# expert access-list advanced adv-acl
AC-FS(config-exp-dacl)# permit a0c8040c ffffffff 38
AC-FS(config-exp-dacl)# show access-lists
expert access-list advanced adv-acl
10 permit a0c8040c ffffffff 38 AC-
FS(config-exp-dacl)# exit
AC-FS(config)# interface gigabitethernet 1/1
AC-FS(config-if)# expert access-group adv-acl in
```

【Verification】 1: Use the show access-lists command to view the configuration information of all ACLs, including all the rules configured under the ACL.

2: Use the show access-lists id command to view the configuration information of the specified ACL, including all the rules configured under the ACL.

3: Use the show access-lists name command to view the configuration information of the specified ACL, including all the rules configured under the ACL.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

12.22remark

Add comment information to ACE in ACL

remark text

Remove ACE comment information

no remark text

【Parameter Description】

Parameter	Description
text	Note Information

【Default Configuration】 ACE has no comment information

【Command Mode】ACL mode

【Default Level】 14

【Usage Guide】Only allow up to 100 characters, not allow 2 comments of the same content in one ACL.

When an ace is deleted, the ace and the corresponding comment information will be deleted together.

【Configuration Example]】1: Add comment information to the ACE in the IP extension ACL numbered 102:

```
AC-FS(config)# ip access-list extended 102
AC-FS(config-ext-nacl)# remark first_remark
```

```
AC-FS(config-ext-nacl)# permit tcp 1.1.1.1 0.0.0.0 2.2.2.2 0.0.0.0
AC-FS(config-ext-nacl)# remark second_remark
AC-FS(config-ext-nacl)# permit tcp 3.3.3.3 0.0.0.0 4.4.4.4 0.0.0.0
AC-FS(config-ext-nacl)# end
AC-FS#
```

【Verification】1: Use the show access-lists command to view the configuration information of all ACLs. Include comment information for ACL rule entries.

2: Use the show access-lists id command to view the configuration information of the specified ACL. Include comment information for ACL rule entries.

3: Use the show access-lists name command to view the configuration information of the specified ACL. Include comment information for ACL rule entries.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

12.23 security access-group

Configuring Interface Security Channels

security access-group { id | name }

delete interface secure channel

no security access-group

【Parameter Description】

Parameter	Description
id	ACL number, assignable range: IP standard ACL (1-99, 1300-1999), IP extended ACL (100-199, 2000-2699) (100-199, 2000-2699), MAC extended ACLs (700-799), expert extended ACLs (2700-2899).
name	ACL Name.

【Default Configuration】 There is no secure channel configuration on the interface.

【Command Mode】 Interface mode

【Default Level】 14

【Usage Guide】If some authentication functions are configured on the device, such as 802.1x or web authentication, users cannot access the external network until they pass the authentication. At this time, if you want some users under a certain interface without authentication, you can To access the external network, you can use this command to configure a secure channel.

【Configuration Example]】1: Configure a secure channel on interface GigaEthernet 1/1, and the corresponding ACL number is 1:

```
AC-FS(config)# interface GigaEthernet 1/1
AC-FS(config-if-GigabitEthernet 1/1)# security access-group 1
```

【Verification】Use the show running command to verify the configuration

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

12.24security global access-group

Configure global secure channel.

security global access-group { id | name }

Delete global secure channel.

no security global access-group

【Parameter Description】

Parameter	Description
id	ACL number, assignable range: IP standard ACL (1-99, 1300-1999), IP extended ACL (100-199, 2000-2699)(100-199, 2000-2699), MAC extended ACLs (700-799), expert extended ACLs (2700-2899).
name	ACL Name.

【Default Configuration】 No global secure channel configuration.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】If some authentication functions are configured on the device, such as 802.1x or web authentication, users cannot access the external network until they pass the authentication. At this time, if you want some users under different interfaces without authentication, you can To access the external network, you can use this command to configure a global secure channel.

【Configuration Example]】1: Configure a global security channel, the corresponding ACL number is 1:

```
AC-FS(config)# security global access-group 1
```

【Verification】Use the show running command to view the global secure channel configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

12.25security uplink enable

Configure the exception port of the global secure channel.

security uplink enable

Cancel the interface global security channel exception port.

no security uplink enable

【Parameter Description】-

【Default Configuration】 The interface is not an exception interface of the global secure channel.

【Command Mode】 Interface mode

【Default Level】 14

【Usage Guide】 Since the global secure channel takes effect on all interfaces, if you want the global secure channel to not take effect on some interfaces, you can configure these interfaces as exception ports of the secure channel.

【Configuration Example]】1: Configure the interface GigaEthernet 1/1 as the exception interface of the global secure channel:

```
AC-FS(config)# interface GigaEthernet 1/1
AC-FS(config-if-GigabitEthernet 1/1)# security uplink enable
```

【Verification】 Use the show running command to view which interfaces are configured as exception interfaces of the global secure channel

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

12.26show access-group

Displays the ACL configuration applied on an interface

show access-group [interface interface-name]

【Parameter Description】

Parameter	Description
interface Interface-name	Specified interface name.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】If you want to check whether an ACL is applied to a specified interface, or to check which interfaces have an ACL applied, you can use this command.

【Configuration Example]】1: Check which interfaces on the device have ACLs applied to, and the direction of application:

```
AC-FS# show access-group
ip access-list  standard  ipstd3  in
Applied On interface GigabitEthernet 0/1.
ip access-list standard ipstd4 out
Applied On interface GigabitEthernet 0/2.
ip access-list extended 101 in
Applied On interface GigabitEthernet 0/3.
ip access-list extended 102 in
Applied On interface GigabitEthernet 0/8.
```

2: Check whether the ACL is applied on the interface GigabitEthernet 0/3, and the direction of the application:

```
AC-FS# show access-group interface GigabitEthernet 0/3
ip access-list extended 101
Applied On interface GigabitEthernet 0/3 in.
```

【Prompt Information】-

【Platform Description】 -

12.27show access-lists

Displays all ACL configurations or the configuration of a specified ACL

show access-lists [id | name] [summary]

【Parameter Description】

Parameter	Description

id	Number of ACL.
name	The name of the ACL.
summary	Summary information of the ACL.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Display the specified ACL configuration information. If no ACL number or name is specified, all ACL configuration information will be displayed.

【Configuration Example]】 1: View the ACL configuration information named "n_acl":

```
AC-FS# show access-lists n_acl
ip access-list standard n_acl
AC-FS# show access-lists 102
ip access-list extended 102
```

2: View all ACL configuration information:

```
AC-FS# show access-lists
ip access-list standard n_acl
ip access-list extended 101
  permit icmp host 192.168.1.1 any log (1080 matches)
  permit tcp host 1.1.1.1 any established
  deny ip any any (80021 matches)
mac access-list extended mac-acl
expert access-list extended exp-acl
ipv6 access-list extended v6-acl
  petmit ipv6 ::192.168.4.12 any (100 matches)
  deny any any (9 matches)
```

【Prompt Information】 -

【Platform Description】 -

12.28 show expert access-group

Displays the expert-level extended ACL configuration applied on the interface.

show expert access-group [interface interface-name]

【Parameter Description】

Parameter	Description
interface Interface-name	Specified interface name.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】Displays the expert-level ACL applied on the interface. If no interface is specified, it displays the expert-level ACL applied on all interfaces.

【Configuration Example]】1: Check whether the expert-level extended ACL is applied on the interface GigabitEthernet 0/2, and the direction of the application

```
AC-FS# show expert access-group interface gigabitethernet 0/2
expert access-group ee in
Applied On interface GigabitEthernet 0/2.
```

【Prompt Information】-

【Platform Description】 -

12.29 show ip access-group

Displays IP Standard and IP Extended ACL configurations applied on an interface

show ip access-group [interface interface-name]

【Parameter Description】

Parameter	Description
interface Interface-name	Specified interface name.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Displays the IP standard and IP extended ACL applied on the interface. If no interface is specified, it displays the IP standard and IP extended ACL applied on all interfaces.

【Configuration Example]】1: Check whether the IP standard and IP extension ACL are applied on the interface GigabitEthernet 0/1, and the direction of application:

```
AC-FS# show ip access-group interface gigabitethernet 0/1ip
access-group aaa in
Applied On interface GigabitEthernet 0/1.
```

【Prompt Information】-

【Platform Description】 -

12.30show ipv6 traffic-filter

Displays IPv6 ACL configuration applied on an interface.

show ipv6 traffic-filter [interface interface-name]

【Parameter Description】

Parameter	Description
interface Interface-name	Specified interface name.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Displays the IPv6 ACL applied on the interface. If no interface is specified, it displays the IPv6 ACL applied on all interfaces.

【Configuration Example]】1: Check whether an IPv6 ACL is applied on interface GigabitEthernet 0/1, and the direction of application:

```
AC-FS# show ipv6 traffic-filter interface gigabitethernet 0/4
ipv6 traffic-filter v6 in
Applied On interface GigabitEthernet 0/4.
```

【Prompt Information】-

【Platform Description】 -

12.31 show mac access-group

Displays the MAC extended ACL applied on the interface.

show mac access-group [interface interface-name]

【Parameter Description】

Parameter	Description
interface Interface-name	Specified interface name.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Displays the extended MAC ACL applied on the interface. If no interface is specified, it displays the extended MAC ACL applied on all interfaces.

【Configuration Example】】 1: Check whether an extended MAC ACL is applied on interface GigabitEthernet 0/3, and the direction of application.

```
AC-FS# show mac access-group interface gigabitethernet 0/3
mac access-group mm in
Applied On interface GigabitEthernet 0/3.
```

【Prompt Information】 -

【Platform Description】 -

13 SCC

13.1 Command Identifier Table

The identifiers used in the following commands can be found in the following command identifier table:

Identifier	Meaning
vlanlist	Authentication-free VLAN list.
interval	Online authentication user detection period.
thredshold	Traffic threshold for online authenticated user detection.

13.2 downstream average-rate burst-rate

Configure the average and burst value of downlink rate-limited traffic.

downstream average-rate avg-threshold burst-rate burst-threshold

Cancel the average and burst value of downlink rate-limited traffic.

no downstream

【Parameter Description】

Parameter	Description
avg-threshold	Speed limit average.
burst-threshold	Speed limit burst value.

【Default Configuration】 None

【Command Mode】 Speed limit strategy configuration mode

【Default Level】 14

【Usage Guide】 The downlink speed limit burst value is not less than the average value.

【Configuration Example】1: Configure user policy, specify rate limit policy name.

```
AC-FS(config)# rate-policy user-rate
AC-FS (config-rate-policy)#downstream average-rate 10 burst-rate 10
```

【Verification】1: Use the show running command to view the downlink policy rules for speed limit configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

13.3 filter-policy

Enter the filter policy configuration mode. filter-policy filter-name Configured in filter policy configuration mode

filter-acl { acl-name | acl-id }

【Parameter Description】

Parameter	Description
filter-name	Filter policy name.
acl-name	The acl-name of the security acl associated with the filtering policy.
acl-id	The acl-id of the security acl associated with the filtering policy.

【Default Configuration】 None

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 The same filtering policy can be applied to different service policies.

【Configuration Example】1: Filter policy.

```
AC-FS(config)# ip access-list extended user_2000 AC-FS(config)#
filter-policy user-filter
AC-FS(config-filter-policy)#filter-acl user_2000
```

【Verification】1: Use the show running command to view the filtering configuration policy.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

13.4 filter-policy apply

Configure the filter policy used.

filter-policy filter-name apply

Use the specified filter policy.

no filter-policy

【Parameter Description】

Parameter	Description
filter-name	Name of the filtering policy used.

【Default Configuration】 None

【Command Mode】 User policy configuration mode

【Default Level】 14

【Usage Guide】 The filter policy name used must be configured first.

【Configuration Example】1: Configure user policy, specify filter policy name.

```
AC-FS(config)# ip access-list extended user_2000
AC-FS(config)# filter-policy user-filter AC-
FS(config-filter-policy)#filter-acl user_2000 AC-
FS (config)# service-policy user-policy
AC-FS (config-service-policy)# filter-policy user-filter apply
```

【Verification】1: Use the show running command to view the filtering policy rules used by the user policy.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

13.5 filter-acl

Configure the security ACL associated with the filter policy.

filter-acl { acl-name | acl-id }

Cancel the configuration of the security acl associated with the filter policy.

no filter-acl

【Parameter Description】

Parameter	Description
acl-name	acl-name of the security acl associated with the filter policy.
acl-id	acl-id of the security acl associated with the filter policy.

【Default Configuration】 None

【Command Mode】 Filter policy configuration mode

【Default Level】 14

【Usage Guide】 The same filtering policy can be applied to different service policies.

【Configuration Example】1: Filter policy.

```
AC-FS(config)# ip access-list extended user_2000
AC-FS(config)# filter-policy user-filter AC-
FS(config-filter-policy)#filter-acl user_2000
```

【Verification】1: Use the show running command to view the security ACLs associated with the filtering configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

13.6offline-detect interval threshold

Configure the online detection function of authenticated users to log off with low traffic or no traffic within a specified time period.

offline-detect interval interval threshold thredshold

Restore the online detection of authenticated users to the default configuration.

default offline-detect

Disable online detection of authenticated users.

no offline-detect

【Parameter Description】

Parameter	Description
interval	Flow detection period, in minutes, in the range [1, 65535] for non-switch products and [6, 65535] for switch products. The value range is [6, 65535] on switch products.
threshold	Flow rate, in bytes, in the range [0, 4294967294]. 0 means None traffic detection.

【Default Configuration】 8 hours no traffic detection offline.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 When the traffic of an authenticated user is lower than a certain value, it is considered that the user is not using the network, the user is offline, and the user is no longer billed. To implement such a function, you can configure the online detection function of authenticated users.

【Configuration Example]】1: If the user's traffic is less than 5kBytes within 5 minutes of configuration, the user will be offline:

```
AC-FS(config)#offline-detect interval 5 threshold 5120
```

【Verification】1: Use the show running command to view the configuration related to the online detection of authenticated users.

【Prompt Information】-

【Common Mistake】-

13.7 rate-policy

Enter the rate limit policy configuration mode.

rate-policy rate-name

Configured in rate limit policy configuration mode

{downstream | upstream } average-rate avg-threshold burst-rate burst-threshold

【Parameter Description】

Parameter	Description
rate-name	Speed limit policy name.
avg-threshold	Speed limit average.
burst-threshold	Speed limit burst value.

【Default Configuration】 None

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 The same rate limit policy can be applied to different service policies.

【Configuration Example】1: Speed limit strategy.

AC-FS(config)# rate-policy user-rate

```
AC-FS (config-rate-policy)#upstream average-rate 10 burst-rate 10
AC-FS (config-rate-policy)#downstream average-rate 10 burst-rate 10
```

【Verification】1: Use the show running command to view the speed limit configuration policy.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

13.8 rate-policy apply

Configure the rate limit policy used.

rate-policy rate-name apply

Use the specified rate limit strategy.

no rate-policy

【Parameter Description】

Parameter	Description
rate-name	Name of the speed limit policy used.

【Default Configuration】 None

【Command Mode】 User policy configuration mode

【Default Level】 14

【Usage Guide】 The name of the speed limit policy used must be configured first.

【Configuration Example】1: Configure user policy, specify rate limit policy name

```
AC-FS(config)# rate-policy user-rate
AC-FS (config-rate-policy)#upstream average-rate 10 burst-rate 10 AC-FS
(config-rate-policy)#downstream average-rate 10 burst-rate 10 AC-FS
(config)# service-policy user-policy
AC-FS (config-service-policy)# rate-policy user-rate apply
```

【Verification】1: Use the show running command to view the rate limit policy rules used by the user policy.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

13.9 service-policy

Enters user policy configuration mode.

service-policy service-name

Use the specified rate limit strategy

rate-policy rate-name apply

【Parameter Description】

Parameter	Description
service-name	User policy name.
rate-name	Name of the speed limit policy used.

【Default Configuration】 None

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 The name of the speed limit policy used must be configured first.

【Configuration Example】1: Configure user policy, specify rate limit policy name.

```
AC-FS(config)# rate-policy user-rate
AC-FS (config-rate-policy)#upstream average-rate 10 burst-rate 10 AC-FS
(config-rate-policy)#downstream average-rate 10 burst-rate 10 AC-FS
(config)# service-policy user-policy
AC-FS (config-service-policy)# rate-policy user-rate apply
```

【Verification】1: Use the show running command to view the user policy configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

13.10 upstream average-rate burst-rate

Configure the average and burst value of upstream rate-limited traffic.

upstream average-rate avg-threshold burst-rate burst-threshold

Cancel the average and burst value of upstream rate-limited traffic.

no upstream

【Parameter Description】

Parameter	Description
avg-threshold	Average speed limit.
burst-threshold	Speed limit burst value.

【Default Configuration】 None

【Command Mode】 Speed limit strategy configuration mode

【Default Level】 14

【Usage Guide】 The upstream speed limit burst value is not less than the average value.

【Configuration Example】1: Configure user policy, specify rate limit policy name.

```
AC-FS(config)# rate-policy user-rate
AC-FS (config-rate-policy)#upstream average-rate 10 burst-rate 10
```

【Verification】1: Use the show running command to view the rate limit configuration uplink policy rules.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

14 PASSWORD-POLICY

14.1password policy life-cycle

Set the password lifetime.

password policy life-cycle days

Removes the password lifetime setting.

no password policy life-cycle

【Parameter Description】

Parameter	Description
days	Password survival period, unit: days, range: 1~65535.

【Default Configuration】 The lifetime of the password is not limited.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 The password lifetime is used to limit the usage time of the user's password. When the password exceeds the lifetime, the system will prompt the user to modify the password the next time the user logs in.

After this function is configured, only the global password (configured through the enable password and enable secret commands) and the local user password (configured through the username name password password command), and the passwords in Line mode are not valid.

【Configuration Example]】1: The following example configures the password lifetime to be 90 days:

```
AC-FS(config)# password policy life-cycle 90
```

【Verification】1: Use the show password policy command to check whether the lifetime of the password is set and the size of the lifetime.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

14.2 password policy min-size

Limit the minimum length of user passwords.

password policy min-size length

Removed limit the minimum length of user passwords.

no password policy min-size

【Parameter Description】

Parameter	Description
length	Specify the minimum length of the passphrase, range: 1~31.

【Default Configuration】 Disable the minimum password length limit, and do not implement the minimum password length limit.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command is used to configure the minimum length limit of the password. If the minimum length limit of the password is not configured, the minimum length limit of the password will not be set when the user sets the password.
After this function is configured, only the global password (configured through the enable password and enable secret commands) and the local user password (configured through the username name password password command), and the passwords in Line mode are not valid.

【Configuration Example]】1: The following example configures a password with a minimum length of 8:

```
AC-FS(config)# password policy min-size 8
```

【Verification】1: Use the show password policy command to check whether the minimum password length is restricted and the restricted minimum password length.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

14.3 password policy no-repeat-times

Limit reuse of passwords that have been configured the last few times.

password policy no-repeat-times times

Remove the restriction to reuse passwords that have been configured the last few times.

no password policy no-repeat-times

【Parameter Description】

Parameter	Description
times	The last few times the password has been configured, range: 1~31.

【Default Configuration】 Do not restrict the reuse of the passwords that have been used several times recently.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 After this function is enabled, the old passwords that the user has used recently will be recorded to form the password history of the user. If the new password set by the user has been used before, the system will give an error message and fail to change the password.

You can configure the maximum number of user password history records. When the number of password history records exceeds the configured maximum number of history records, the new password history record will overwrite the user's oldest password history record.

After this function is configured, only the global password (configured through the enable password and enable secret commands) and the local user password (configured through the username name password password command), and the passwords in Line mode are not valid.

【Configuration Example]】 1: The following example configuration restricts the reuse of the last 5 configured passwords:

```
AC-FS(config)# password policy no-repeat-times 5
```

【 Verification 】 1: Use the show password policy command to check whether to limit the reuse of the passwords that have been configured recently and the maximum number of password history records.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

14.4password policy strong

Enable strong password detection.

password policy strong

Disable strong password detection.

no password policy strong

【Parameter Description】-

【Default Configuration】 Disable strong password detection, and do not perform strong password detection when users set a password.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】After enabling this function, you can create an alarm for the following password configurations that do not meet the password strength policy when creating a new user:

1. The password with the same name as the account;

2. Simple passwords containing only characters or numbers.

After this function is configured, only the global password (configured through the enable password and enable secret commands) and the local user password (configured through the username name password password command), and the passwords in Line mode are not valid.

【Configuration Example]】1: The following example configures strong password checking:

```
AC-FS(config)# password policy strong
```

【Verification】1: Use the show password policy command to check whether the strong password detection function is enabled.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

14.5 service password-encryption

Set password encryption storage.

service password-encryption

Delete password encryption storage settings.

no service password-encryption

【Parameter Description】-

【Default Configuration】 The password is not encrypted and stored.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】Before password encryption storage is set, all passwords used in the user configuration process are displayed and stored in plain text, unless cipher text is used for configuration directly. For security reasons, the password encryption storage function can be turned on. After this function is turned on, various passwords set by the user will become ciphertext when the show running-config or write is performed to save; if the password encryption storage function is turned off again, it has become Ciphertext passwords are not restored to plaintext.

【Configuration Example]】1: The following example sets the password to be encrypted and stored:

```
AC-FS(config)# service password-encryption
```

【Verification】1: Use the show password policy command to check whether the password encryption storage function is enabled.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

14.6show password policy

View the password security policy information set by the user.

show password policy

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】 Use this command to view the password security policy information set on the device.

【Configuration Example]】1: View the password security policy information set by the user.

```
AC-FS#show password policy
Global password policy configurations:
 Password encryption:                Enabled
 Password strong-check:              Enabled
 Password min-size:                  Enabled (6 characters)
 Password life-cycle:                Enabled (90 days)
 Password no-repeat-times:           Enabled (max history record: 5)
```

Field Description:

Field	Description
Password encryption	Whether the password is stored encrypted.
Password strong-check	Whether to turn on strong password checking.
Password min-size	Limit the minimum length of the password.
Password life-cycle	Limit the password survival period.
Password no-repeat-times	Restrict reuse of the last few used passwords.

【Prompt Information】-

【Platform Description】 -

15 SSH

15.1crypto key generate

Generate server-side public key

crypto key generate { rsa | dsa }

【Parameter Description】

Parameter	Description
rsa	Generate RSA key.
dsa	Generate DSA key.

【Default Configuration】 By default, SSH Server does not generate a public key.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 When you need to open the SSH Server service, use this command to generate the public key of the SSH server. Run the enable service ssh-server command at the same time to enable the SSH Server function. SSH 1 uses RSA keys; SSH 2 uses RSA or DSA keys. Therefore, if RSA keys are currently generated, both SSH1 and SSH2 will work; if only DSA keys are generated, only SSH2 will work.

Although a client can only use one of the DSA and RSA public key algorithms to authenticate the server during a connection process, due to the different public key algorithms supported by different clients, in order to ensure that the client can successfully log in to the server, it is recommended to Two key pairs, DSA and RSA, are generated on the server.

The minimum length of the modulus of the RSA host key is 512 bits, the minimum length of the modulus of the DSA host key is 360 bits, and the maximum length of the modulus of both is 2048 bits. In SSH2, some clients (such as the SCP file transfer client) require that the key length generated by the server must be greater than or equal to 768 bits. It is recommended that users specify the modulus of the host key as 768 bits or greater when configuring RSA and DSA host keys.

When deleting a key, there is no command no crypto key generate, but the key is deleted by the command crypto key zeroize.

【Configuration Example]】1: Generate the rsa key of the server.

```
AC-FS# configure terminal
AC-FS(config)# crypto key generate rsa
```

【Verification】1: Use the show crypto key mypubkey rsa command to confirm whether the rsa has been generated by checking whether

the public part of the rsa key exists.

【Prompt Information】1: If the rsa key of the server is generated for the first time, it will prompt you to select the number of key digits and the information about the success or failure of the generation.

```
AC-FS(config)#crypto key generate rsa
Choose the size of the rsa key modulus in the range of 512 to 2048
```

```
and the size of the dsa key modulus in the range of 360 to 2048 for your Signature Keys. Choosing a key modulus greater
than 512 may take
a few minutes.
How many bits in the modulus [512]:
/ rsa key generation failurePrompt Imformation
% Generating 512 bit RSA1 keys          [ok]
% Generating 512 bit RSA keys[ok]
// rsa key generation failurePrompt Imformation
% Generating 512 bit RSA1 keys          [fail]
% Generating 512 bit RSA keys[fail]
```

2: If the rsa key already exists on the server, it will prompt whether to replace it. If it is, it will prompt to re-select the number of key digits and generate success or failure information, otherwise, exit directly.

```
AC-FS(config)#crypto key generate rsa
% You already have RSA keys.
% Do you really want to replace them? [yes/no]:yes
Choose the size of the rsa key modulus in the range of 512 to 2048
and the size of the dsa key modulus in the range of 360 to 2048 for your Signature Keys. Choosing a key modulus greater
than 512 may take
a few minutes.
How many bits in the modulus [512]:
```

3: If the input rsa key number is not within the range of 512~2048, it will prompt that the input number is wrong and prompt to re-enter.

```
AC-FS(config)#crypto key generate rsa
Choose the size of the rsa key modulus in the range of 512 to 2048
and the size of the dsa key modulus in the range of 360 to 2048 for your Signature Keys. Choosing a key modulus greater
than 512 may take
a few minutes.
How many bits in the modulus [512]:360 sshd: rsa key in the range of 512 to 2048 How many bits in the modulus [512]:2590
sshd: bad data bits
How many bits in the modulus [512]:
```

【Common Mistake】-

【Platform Description】 -

15.2crypto key zeroize

Delete the public key on the SSH server side.

crypto key zeroize { rsa | dsa }

【Parameter Description】

Parameter	Description
rsa	Delete RSA key.
dsa	Delete DSA key.

【Default Configuration】-

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to delete the public key of the server. After the key is deleted, the status of the SSH Server becomes DISABLE. If you need to shut down the SSH Server, you need to execute the no enable service ssh-server command.

【Configuration Example]】1: Delete the rsa key of the server.

```
AC-FS# configure terminal
AC-FS(config)# crypto key zeroize rsa
```

【Verification】1: Use the show crypto key mypubkey rsa command to confirm whether the rsa has been deleted by checking whether the public part of the rsa key exists.

【Prompt Information】1: If the rsa key already exists on the server, it will prompt whether to delete the rsa key.

```
AC-FS(config)#crypto key zeroize rsa
% Keys to be removed
% All router certs issued using these keys will also be removed.
Do you really want to remove these keys? [yes/no]:yes
*Jan 16 06:52:57: %P17050-7-DEBUG: sshd: delete key file /rsa_private.bin
*Jan 16 06:52:57: %P17050-7-DEBUG: sshd: delete key file /rsa1_private.bin
```

2: If the rsa key is not generated, it will prompt that the rsa key does not exist.

```
AC-FS(config)#crypto key zeroize rsa
% The specified RSA keypair does not exist.
```

【Common Mistake】 1: Use the no and default command prefix to delete the key, then the key will not be deleted.

【Platform Description】 -

15.3 disconnect ssh

Disconnect an established SSH connection session.

disconnect ssh [vty] session-id

【Parameter Description】

Parameter	Description
vty	Established vty connection.
session-id	The established SSH connection session number, in the range of 0 to 35.

【Default Configuration】-

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】 Disconnect the established SSH connection by entering the specified SSH connection session number. Or enter the

specified VTY connection session number to disconnect the specified SSH connection. Only SSH type connections can be disconnected.

【Configuration Example】1: Enter the specified SSH connection session number to disconnect the established SSH connection.

```
AC-FS# disconnect ssh 1
```

2: Enter the specified VTY connection session number to disconnect the specified SSH connection.

```
AC-FS# disconnect ssh vty 1
```

【Verification】1: Use the show ssh command to check whether the specified SSH connection has been disconnected.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

15.4 disconnect ssh-session

Disconnect pending SSH Client connections.

disconnect ssh-session session-id

【Parameter Description】

Parameter	Description
session-id	Suspended SSH Client connection session number.

【Default Configuration】-

【Command Mode】 Normal user mode

【Default Level】1

【Usage Guide】 Disconnect the specified SSH Client by entering the specified SSH Client connection session number.

【Configuration Example】1: Enter the specified SSH Client connection session number and disconnect the specified SSH Client connection.

```
AC-FS# disconnect ssh-session 1
```

【Verification】1: Use the show ssh-session command to check whether the specified SSH Client connection has been disconnected.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

15.5ip scp server enable

Turn on the SCP server function on the network device.

ip scp server enable

Turn off the SCP server function.

no ip scp server enable

【Parameter Description】-

【Default Configuration】 The default setting does not enable the SCP server function.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】Users can directly download files on network devices, and upload local files to network devices. At the same time, all interactive data is transmitted in cipher text, which has the characteristics of authentication and security.

【Configuration Example】1: Enable scp function.

```
AC-FS# configure terminal
AC-FS(config)# ip scp server enable
```

【Verification】1: Use the show ip ssh command to check whether the SCP server function is enabled.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

15.6 ip scp server topdir

Set SCP server file upload and download paths.

ip scp server topdir {flash:/path | flash2:/path | usb0:/path | usb1:/path | sd0:/path | sata0:/path | tmp:/path }

Restore the SCP server file transfer path to the default value.

no ip scp server topdir

【Parameter Description】

Parameter	Description
flash	Transfer file path is selected in Extended FLASH, by default the file transfer path is flash:/.
flash2	The transfer file path is selected in the extended FLASH2, this option is required if the device has a data2 partition to be supported.
usb0	The transfer file path is selected in USB0, this option requires the device to have 1 USB port This option is supported when the device has 1 USB interface and is plugged into an extended USB device.
usb1	Transfer file path selection in USB1, this option requires the device to have 2 USB ports This option is supported when the device has 2 USB ports and an extended USB device is inserted.
sd0	Transfer file path in SD card, this option is supported when the device has an SD card interface This option is supported when the device has an SD card interface and is inserted into an extended SD card device.
sata0	Transfer file path to the hard disk, this option is supported when the device has a SATA partition.
tmp	The transfer file path is selected in the temporary tmp/vsd/ directory.

【Default Configuration】 The default file transfer path is flash:/.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Users can use this command to modify the file transfer path, including file upload and file download.

【Configuration Example]】1: Modify the file transfer path to the tmp/vsd directory.

```
AC-FS# configure terminal
AC-FS(config)# ip scp server topdir tmp:/
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

15.7 ip ssh access-class

Set ACL filtering rules for SSH Server.

ip ssh access-class { access-list-number | access-list-name }

Delete the ACL filtering rules of SSH Server.

no ip ssh access-class

【Parameter Description】

Parameter	Description
access-list-number	ACL numbering, assignable range: IP Standard ACL (1-99, 1300-1999); IP Extended ACLs (100-199, 2000-2699).
access-list-name	ACL name.

【Default Configuration】-

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Users can use this command to perform ACL filtering on all SSH connections. The ACL filtering under line only performs

ACL filtering on specific lines, while the SSH ACL filtering rules can perform ACL filtering on all SSH connections.

【Configuration Example]】 1: Configure all SSH connections to be filtered by the ACL named testv4.

```
AC-FS# configure terminal
AC-FS(config)# ip ssh access-class testv4
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

15.8 ip ssh authentication-retries

Set the number of re-authentication times for SSH Server user authentication.

ip ssh authentication-retries retry times

Restore to default settings. ,

no ip ssh authentication-retries

【Parameter Description】

Parameter	Description
retry times	Configure the number of re-authentication of user authentication, the value range is 0~5.

【Default Configuration】 The number of re-authentication is 3 times.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command configures the number of re-authentication times for SSH Server to perform user authentication. When the number of re-authentications configured on the SSH Server is exceeded, and no authentication is successful, the user authentication is

considered to have failed.

【Configuration Example】 1: Set the number of re-authentication times for user authentication to 2.

```
AC-FS# configure terminal
AC-FS(config)# ip ssh authentication-retries 2
```

【Verification】 1: Use the show ip ssh command to view the configuration information of the number of re-authentication times for SSH Server user authentication.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

15.9ip ssh cipher-mode

Set the encryption mode supported by SSH Server.

ip ssh cipher-mode { cbc | ctr | others }

Use the no option of this command to set the encryption mode supported by SSH Server to the default setting.

no ip ssh cipher-mode

【Parameter Description】

Parameter	Description
cbc	The encryption mode supported by SSH Server is cbc mode (cipher block chaining mode), and the corresponding encryption algorithms are: DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, AES-256-CBC and Blowfish-CBC.
ctr	Configure the encryption mode supported by SSH Server as ctr mode (counter mode), and its corresponding algorithms are. AES128-CTR, AES192-CTR, AES256-CTR.
others	Configure the encryption mode supported by SSH Server to others, and the corresponding encryption algorithm is: RC4

【Default Configuration】 By default, the encryption mode supported by SSH Server is compatibility mode (supports cbc, ctr and other classes).

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command configures the encryption mode supported by SSH Server.

Among FS devices, the encryption algorithms supported by SSHv1 Server are: DES-CBC, 3DES-CBC, Blowfish-CBC; the encryption algorithms supported by SSHv2 Server are: AES128-CTR, AES192-CTR, AES256-CTR, DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, AES-256-CBC, Blowfish-CBC, RC4. Among these encryption algorithms, it can be classified into three different encryption modes: "cbc" (cipher block chaining mode), "ctr" (counter mode: counter mode) and others.

With the continuous development of cryptography, the encryption algorithms of "cbc" and "others" encryption modes have been proved to be able to be cracked in a limited time. Therefore, in some organizations or units with high security requirements, the security level of SSH Server can be improved by configuring the encryption mode supported by SSH Server to "ctr" mode.

【Configuration Example】1: Set the encryption mode supported by SSH Server to ctr mode.

```
AC-FS# configure terminal
AC-FS(config)# ip ssh cipher-mode ctr
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

15.10ip ssh hmac-algorithm

Set the message authentication algorithm supported by SSH Server.

ip ssh hmac-algorithm { md5 | md5-96 | sha1 | sha1-96 }

Use the no option of this command to restore the message authentication algorithms supported by SSH Server to the default settings.

no ip ssh hmac-algorith

【Parameter Description】

Parameter	Description

md5	Configure the message authentication algorithm supported by SSH Server to be md5.
md5-96	Configure the message authentication algorithm supported by SSH Server to be md5-96.
sha1	Configure the message authentication algorithm supported by SSH Server to be sha1.
sha1-96	Configure the message authentication algorithm supported by SSH Server to be sha1-96.

【Default Configuration】 By default, the message authentication algorithms supported by SSH Server are: SSHv1 does not support, SSHv2 supports 4 kinds (MD5, SHA1, SHA1-96, MD5-96).

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command configures the message authentication algorithm supported by SSH Server.

Among FS devices, the SSHv1 Server does not support message authentication algorithms; the message authentication algorithms supported by the SSHv2 Server are: md5, sha1, sha1-96, and md5-96. Users can choose the message authentication algorithm supported by SSH Server according to actual needs.

【Configuration Example]】1: Set the message authentication algorithm supported by SSH Server to sha1.

```
AC-FS# configure terminal
AC-FS(config)# ip ssh hmac-algorithm sha1
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

15.11 ip ssh key-exchange

Set the DH key exchange algorithm supported by SSH Server.

ip ssh key-exchange { dh_group_exchange_sha1 | dh_group14_sha1 | dh_group1_sha1 }

Use the no option of this command to restore the DH key exchange algorithm supported by SSH Server to the default settings.

no ip ssh key-exchange

【Parameter Description】

Parameter	Description
dh_group_exchange_sha1	Configure DH key exchange algorithm as diffie-hellman-group-exchange-sha1. key length default The key length is 2048 bytes and is not configurable.
dh_group14_sha1	Configure the DH key exchange algorithm as diffie-hellman-group14-sha1. the key length is 2048 bytes. The key length is 2048 bytes.
dh_group1_sha1	Configure the DH key exchange algorithm as diffie-hellman-group1-sha1 with a key length of 1024 bytes. The key length is 1024 bytes.

【Default Configuration】 By default, the DH key exchange algorithms supported by SSH Server are: SSHv1 does not support, SSHv2 supports 3 types. (diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, diffie-hellman-group1-sha1).

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command configures the DH key exchange algorithm supported by SSH Server.

Among FS devices, the SSHv1 Server does not support the DH key exchange algorithm; the DH key exchange algorithms supported by the SSHv2 Server are: diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, diffie-hellman-group1 -sha1. Users can choose the DH key exchange algorithm supported by SSH Server according to actual needs.

【Configuration Example]】1: Set the DH key exchange algorithm supported by SSH Server to diffie-hellman-group14-sha1.

```
AC-FS# configure terminal
AC-FS(config)# ip ssh key-exchange dh_group14_sha1
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

15.12ip ssh peer

Associate the client's public key file with the user name. When the client logs in for authentication, specify the public key file to be used by the user name.

ip ssh peer username public-key { rsa | dsa } filename

Disassociates the client's public key file from the username.

no ip ssh peer username public-key { rsa | dsa } filename

【Parameter Description】

Parameter	Description
username	User name.
filename	Public key file name.
rsa	public-key type is rsa.
dsa	public-key type is dsa.

【Default Configuration】-

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Set the RSA and DSA public key files associated with user test.

```
AC-FS# configure terminal
AC-FS(config)# ip ssh peer test public-key rsa flash:rsa.pub AC-
FS(config)# ip ssh peer test public-key dsa flash:dsa.pub
```

【Verification】-

【Prompt Information】1: If the associated public key file exceeds the maximum number of 1024 supported by SSH Public Key, it will prompt out of range.

```
AC-FS(config)# ip ssh peer test public-key rsa flash:rsa.pub
%% Too many public-keys, system support max public key 1024
```

2: If the associated public key file name is entered, it will prompt that the public key file name is invalid.

```
AC-FS(config)#ip ssh peer test public-key rsa flash:
% Invalid file name
```

【Common Mistake】-

【Platform Description】 -

15.13 ip ssh port

Set the listening port number of SSH Server.

ip ssh port port

Restore the listening port number setting of the SSH Server to the default setting.

no ip ssh port ip ssh port 22

【Parameter Description】

Parameter	Description
port	Configure the listening port number for SSH Server with a value range from 1025 to 65535.

【Default Configuration】-

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Modify the listening port number of SSH Server to 10000.

```
AC-FS# configure terminal
AC-FS(config)# ip ssh port 10000
```

【Verification】1: Use the show ip ssh command to view the configuration information of the listening port number of the SSH Server.

【Prompt Information】 1: If the configured port number is the same as the current value, it will prompt that the port number is already the value that needs to be configured.

```
AC-FS(config)# ip ssh port 22
% SSH tcp-port has been 22
```

2: If the configured port number is already in the listening state, it will prompt that the port number is already in the listening state, please use another port number, and the current device still uses the old port number.

```
AC-FS(config)# ip ssh port 10000
% SSH open tcp-port(10000) failed, please use another tcp-port,otherwise the system will use the old
tcp-port(22)!
```

3: If the configured port number fails to start listening, it will prompt that the port number configuration failed.

```
AC-FS(config)# ip ssh port 10000
% SSH change to tcp-port(10000) fail!
```

4: If the configured port number is successful, it will prompt that the port number is configured successfully.

```
AC-FS(config)# ip ssh port 10000
% SSH change to tcp-port(10000) success!
```

【Common Mistake】-

【Platform Description】 -

15.14 ip ssh source-interface

Specifies the source interface of the SSH Client.

ip ssh source-interface interface-name

Clear the source interface configuration of the SSH Client.

no ip ssh source-interface

【Parameter Description】

Parameter	Description
interface-name	Specifies that the IP address above the interface will be the source address of the SSH Client.

【Default Configuration】 By default, SSH protocol packets will use the source address of the destination address as the source address of the packet.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command is used to specify the IP address on the interface as the global source address of the SSH Client connection. When using the ssh command to log in to an SSH server, if the source interface or source address is not separately specified for the SSH connection, you can use this command to implement this configuration. Use the no ip ssh source-interface command to restore the settings to default.

【Configuration Example]】1: The following example command specifies the IP address on the Loopback 1 interface as the source address of the global SSH connection:

```
AC-FS(config)# ip ssh source-interface Loopback 1
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

15.15ip ssh time-out

Set the user authentication timeout period for SSH Server.

ip ssh time-out time

Restore the user authentication timeout setting to the default setting.

no ip ssh time-out

【Parameter Description】

Parameter	Description

time	Configure the timeout time for user authentication with a value range of 1 to 120s in seconds.

【Default Configuration】 The timeout period is 120s.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command configures the timeout period for SSH Server to perform user authentication. Timing starts from the acceptance of the user connection request, when the authentication is not successful for more than 120s, the authentication timeout is considered to have failed.

【Configuration Example】1: Configure the timeout to 100s:

```
AC-FS# configure terminal
AC-FS(config)# ip ssh time-out 100
```

【Verification】1: Use the show ip ssh command to view the timeout configuration information of SSH Server user authentication.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

15.16ip ssh version

Set the version of SSH Server.

ip ssh version { 1 | 2 }

Restore the version settings to the default settings.

no ip ssh version

【Parameter Description】

Parameter	Description

1	Configuration SSH Server supports only client connection requests for SSH2.
2	Configuration SSH Server supports client connection requests for SSH1.

【Default Configuration】 Compatible with SSH version 1 and 2.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command is used to configure the SSH connection protocol version supported by SSH Server. By default, the versions supported by SSH Server are compatible with SSH1 and SSH2, and clients using SSH1 or SSH2 can connect. If version 1 or 2 is set, only SSH clients of the corresponding version are allowed to connect.

【Configuration Example]】1: Set to use only version 2:

```
AC-FS# configure terminal
AC-FS(config)# ip ssh version 2
```

【Verification】1: Use the show ip ssh command to view the SSH protocol version currently supported by the SSH Server.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

15.17 ipv6 ssh access-class

Set IPv6 ACL filtering rules for SSH Server.

ipv6 ssh access-class accessv6-list-name

Delete the IPv6 ACL filtering rule for SSH Server.

no ipv6 ssh access-class

【Parameter Description】

Parameter	Description

accessv6-list-name	The IPv6 ACL name.

【Default Configuration】-

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Users can use this command to perform IPv6 ACL filtering on all SSH connections. The IPv6 ACL filtering under line only performs IPv6 ACL filtering on specific lines, while the SSH IPv6 ACL filtering rules can perform IPv6 ACL filtering on all SSH connections.

【Configuration Example]】1: Configure all SSH connections to be filtered by the IPv6 ACL named testv6.

```
AC-FS# configure terminal
AC-FS(config)# ipv6 ssh access-class testv6
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

15.18 show crypto key mypubkey

Displays information for the public key portion of the SSH Server public key.

show crypto key mypubkey { rsa | dsa }

【Parameter Description】

Parameter	Description
rsa	Displays the DSA key.
dsa	Displays the RSA key.

【Command Mode】 Privileged user mode, global configuration mode

【Default Level】 14

【Usage Guide】 Displays the information of the public key part of the generated SSH Server public key. Including: key generation time, key name, part of the public key and other information.

【Configuration Example]】1: Display the information of the public key part of the generated SSH Server public key RSA.

```
AC-FS(config)#show crypto key mypubkey rsa
% Key pair was generated at: 7:1:25 UTC Jan 16 2013
 Key name: RSA1 private
 Usage: SSH Purpose Key
 Key is not exportable.
 Key Data:
        AAAAAwEA AQAAAEEA 2m6H/J+2 xOMLW5MR 8tOmpW1I XU1QItVN mLdR+G7O Q1Okz+4/
        /IgYROge 1sZNg32u dFEifZ6D zfLySPqC MTWLfw==

% Key pair was generated at: 7:1:25 UTC Jan 16 2013
 Key name: RSA private
 Usage: SSH Purpose Key
 Key is not exportable.
 Key Data:
        AAAAAwEA AQAAAEEA OE5w2HOk v744uTIR yZBd/7AM 8pLItnW3 XH3LhEEi BbZGZvn3
        LEYYfQ9s pgYLOZQf SOs/GYOX gJOMsc6z i8OAkQ==
```

Field Description:

Field	Instruction
Key pair was generated at	Open the key section.
Key name	Key usage instructions.
Usage	Key name.
Key Data	Key generation time.

【Prompt Information】-

【Platform Description】 -

15.21 show ssh-session

Displays information about each instance of the established SSH Client instance.

show ssh-session

【Parameter Description】-

【Command Mode】 Normal user mode

【Default Level】1

【Usage Guide】Displays the information of each instance of the established SSH Client instance, including: the VTY number occupied by the connection, the SSH version number, and the server address.

【Configuration Example】1: Display the connection information of the established SSH Client session.

```
AC-FS#show ssh-session
Connect No.   SSH Version   Server Address
-----------   -----------   --------------
0             2.0           192.168.23.122
1             1.5           192.168.23.122
```

【Prompt Information】-

【Platform Description】 -

15.22ssh

In normal user mode, use the ssh command to establish an encrypted session to a remote network device.

ssh [oob] [-v { 1 | 2 }] [-c { 3des | aes128-cbc | aes192-cbc | aes256-cbc | aes128-ctr | aes192-ctr | aes256-ctr }] [-l username] [-m { hmac-md5-96 | hmac-md5-128 | hmac-sha1-96 | hmac-sha1-160 }] [-p port-num] { ip-addr | hostname } [via mgmt-name] [/ source { ip A.B.C.D | ipv6 X:X:X:X::X | interface interface-name }] [/vrf vrf-name]

【Parameter Description】

Parameter	Description
oob	Remote connection to the SSH server via out-of-band communication (generally through the MGMT interface), only at
-v	This option is not available when the device has the MGMT management port ● 1 – Use SSHv1 to connect. ● 2 – Connect using SSHv2.

-c { 3des | aes128-cbc | aes192-cbc | aes256-cbc | aes128-ctr | aes192-ctr | aes256-ctr }	Optional) Specifies the data encryption algorithm. The optional types are: Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), or Advanced Encryption Standard (AES). The Advanced Encryption Standard (AES) algorithm can support six types depending on the key length and mode: aes128-cbc (128-bit key), aes192-cbc (192-bit key), aes256-cbc (256-bit key) , aes128-ctr (128-bit key), aes192-ctr (192-bit key), aes256-ctr (256-bit key). ● If the user does not specify the -c option, during algorithm negotiation, a list of all algorithms supported by the SSH client will be sent to the server. ● If the user specifies the -c option, during algorithm negotiation, the SSH client will only send the encryption algorithm specified by the user to the server. At this time, if the server does not support the encryption algorithm specified by the user, the connection will be closed.
-l username	(Required) Specify the login user name.
-m { hmac-md5-96 | hmac-md5-128 | hmac-sha1-96 | hmac-sha1-160 }	Optional) Specifies a Hash Message Authentication Code (HMAC) algorithm. ● SSHv1 does not support HMACs. If the user specifies both SSHv1 and HMACs, the HMACs are simply ignored. ● If the user does not specify the -m option, during algorithm negotiation, a list of all algorithms supported by the SSH client will be sent to the server. ● If the user specifies the -m option, during algorithm negotiation, the SSH client will only send the HMAC algorithm specified by the user to the server. At this time, if the server does not support the HMAC algorithm specified by the user, the connection will be closed.
-p port-num	(Optional) Specifies the port number to expect when connecting to the remote server. By default, the port number is 22.
ip-addr | hostname	(Required) Specifies the IPv4/IPv6 address or hostname of the remote server.
via mgmt-name	MGMT port to use when specifying the oob option.
/source	Specify the source IP or source interface used by the SSH Client.
ip A.B.C.D	Specifies the source IPV4 address used by the SSH Client.
ipv6 X:X:X:X::X	Specifies the source IPV6 address used by the SSH Client.
interface interface-name	Specifies the source interface used by the SSH Client.
/vrf vrf-name	Specifies the VRF routing table to query.

【Default Configuration】 -

【Command Mode】 Normal user mode

【Default Level】1

【Usage Guide】 The ssh command is used to establish a secure, encrypted connection from the current device (as an SSH client) to another device (as an SSH server) or other server that supports SSHv1 or SSHv2. This connection provides a mechanism similar to a Telnet connection, except that all transmissions over this connection are encrypted. Based on authentication and encryption, SSH Client will establish a secure connection over an insecure network.

SSHv2 can support the following AES advanced encryption algorithms: ase128-cbc, aes192-cbc, aes256-cbc, ase128-ctr, aes192-ctr, and aes256-ctr.

SSHv1 does not support the HMAC authentication code algorithm.

If the user specifies an unmatched encryption algorithm or authentication algorithm while selecting the SSH version number, the unmatched algorithm will be ignored when establishing a connection.

【Configuration Example]】1: From the current device, log in to the device 192.168.23.122 that supports the remote SSH server with the username admin via SSH:

```
AC-FS#ssh -l admin 192.168.23.122
```

2: From the current device, use SSHv2, preferably aes128-cbc as the encryption algorithm and hmac-md5-128 as the authentication algorithm, log in to the device 192.168.23.122 that supports the SSH server remotely with the username admin:

```
AC-FS#ssh -v 2 -c aes128-cbc  -m hmac-md5-128 -l admin 192.168.23.122
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

15.23 ssh-session

Resume an established SSH Client session connection.

ssh-session session-id

【Parameter Description】

Parameter	Description

session-id	An established SSH Client session connection index.

【Default Configuration】-

【Command Mode】 Normal user mode

【Default Level】1

【Usage Guide】 This command is used to restore the connection using the established SSH Client session. When an SSH Client session connection is initiated using the ssh command, the hotkey (ctrl+shift+6 x) can be used to temporarily exit the connection. If the connection needs to be restored, it can be restored using the ssh-session command. At the same time, if the connection has been established, you can use the show ssh-session command to view the established connection information.

【Configuration Example]】1: Restore the established SSH Client session connection.

```
AC-FS# ssh-session 1
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

16 CONTENT-AUDIT

16.1 app-audit

Enable the optimization audit function of application blocking and set the interval time.

app-audit optimize-cache [time]

Turn off the optimized auditing function of application blocking.

no app-audit optimize-cache

Enable application control auditing to optimize blocking of TCP connections, that is, actively send rst packets to disconnect connections.

app-audit optimize-deny

Disable the optimized blocking function of TCP connections by application control auditing.

no app-audit optimize-deny

【Parameter Description】

Parameter	Description
time	The Parameter is built in seconds, and after opening the function, without repeatedly auditing the same IP in time time the same application blocking action.

【Default Configuration】 It is enabled by default.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 1: After the optimization audit function is enabled, the same application blocking action of the same IP within a certain period of time will not be audited repeatedly. The default time length is 300s, and the range is 5~1800 seconds.

2: For TCP flow, there are two ways to apply blocking: one is to directly lose packets, and the other is to actively disconnect by sending rst packets. These two ways can be optimized to block configuration switching.

【Configuration Example]】1: Within the specified 120s, the duplicate application blocking of the same IP will not be audited.

```
AC-FS# configure terminal
AC-FS(config)# app-audit optimize-cache 120 AC-
FS(config)# end
```

2: Disable the optimization blocking function of application control auditing.

```
AC-FS#  configure  terminal AC-FS(config)#
no app-audit optimize-deny
AC-FS(config)# end
```

【Verification】 Use the show running-config command to view the configuration status.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 MSC products do not support, other gateway series products support.

16.2 app-rule

Delete all application control audit rules under the policy group.

app-rule delete-all

Exchange the priority of access control rules.

app-rule priority-swap rule-id1 rule-id2

Add application control audit rules to the content audit policy group.

app-rule rule-id time-range time-name app-group app-group-name action { permit | deny } [audit] [vpn] [vip] [comment comment-string]

Delete application control audit rules.

no app-rule rule-id

【Parameter Description】

Parameter	Description
rule-id1	The Description of the rule.

rule-id2	Application group name that the rule wants to control.
rule-id	Time object name representing the time period when the rule takes effect.
time-name	ID identification of the rule, value range (1~200), and a rule capacity of 200.
app-group-name	The ID of Rule 2 where the priority is to be exchanged.
comment-string	The ID of Rule 1 where the priority is to be exchanged.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Content audit policy group configuration mode

【Default Level】 14

【Usage Guide】 1: The rule-id of a rule is not allowed to be repeated in the same content audit policy group, but is allowed to be repeated in different content audit policy groups.

2: The access control rules in a content audit policy group have corresponding priorities, and the rule assigned last has the highest priority.

3: The time-name and app-group-name associated with the rule may not exist, and the rule will not take effect at this time.

4: When configured to allow application access and auditing, restrictions will be imposed to optimize audit records. In fact, no auditing is performed in this case.

5: The swap priority command is used to swap the priorities of two access control rules. After running this command, you can see that the order of the two rules has changed in show running-config, but the order of the two rules will not appear in show running-config. Order.

【Configuration Example]】 1: Delete all application control audit rules in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# app-rule delete-all
AC-FS(cont-plcy-config)# end
```

2: The priority of the application control audit rule 10 and rule 20 in the exchange policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# app-rule priority-swap 10 20
AC-FS(cont-plcy-config)# end
```

3: Add an application control audit rule to the policy group policyA, filter users for video playback and P2P download, and audit the corresponding filtering information.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# app-rule 2 time-range any direction double app-group VideoAndP2PGroup action deny audit comment DenyVideoAndP2P
AC-FS(cont-plcy-config)# end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】1: If the configured rule-id already exists, a prompt will be given.

```
AC-FS(config)# app-rule 2 time-range any direction double app-group VideoAndP2PGroup action deny audit comment DenyVideoAndP2P
Rule 2 already exists, please delete it first
```

【Common Mistake】-

【Platform Description】 MSC products do not support, other gateway series products support.

16.3class

Add the contained URL categories to the URL object.

class class-name

Deletes the URL category contained in the URL object.

no class class-name

【Parameter Description】

Parameter	Description
class-name	The name of the URL classification, can be the user custom URL classification or the system URL classify.The maximum length is 40 bytes.

【Default Configuration】 There is no configuration by default.

【Command Mode】 URL object configuration mode

【Default Level】 14

【Usage Guide】 1: The URL object allows to include system URL categories and user-defined URL categories.

2: The URL object allows to associate non-existing URL categories.

【Configuration Example]】1: Add a URL category named classA to the URL object objA.

```
AC-FS# configure terminal AC-
FS(config)# url-object objA AC-
FS(url-obj-config)# class classA
AC-FS(url-obj-config)# end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 All gateway series products are supported.

16.4clear content-audit statistics

Clear real-time statistics for content auditing.

clear content-audit statistics

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to clear the real-time statistics of content auditing.

【Configuration Example]】1: Clear the real-time statistics of content auditing.

```
AC-FS#clear content-audit statistics
```

【Prompt Information】-

【Platform Description】 All gateway series products are supported.

16.5comment

Add a Description to a URL category or URL object.

comment comment-string

Delete the Description from the URL category or URL object.

no comment

【Parameter Description】

Parameter	Description
comment-string	Description for URL classification or URL object with up to 100 characters.

【Default Configuration】 There is no configuration by default.

【Command Mode】 URL object configuration mode, URL classification configuration mode

【Default Level】 14

【Usage Guide】 Description is usually used to describe the purpose of URL category or URL object.

【Configuration Example]】 1: Add a Description to the URL object objA.

```
AC-FS# configure terminal AC-
FS(config)# url-object objA
AC-FS(url-obj-config)# comment OBJA-COMMENT
AC-FS(url-obj-config)# end
```

2: Add a Description to the URL category classA.

```
AC-FS# configure terminal AC-
FS(config)# url-class classA
AC-FS(url-cls-config)# comment CLASSA-COMMENT
AC-FS(url-cls-config)# end
```

【Verification】 Use the show running-config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 All gateway series products are supported.

16.6 content-audit write-db

Turn on the switch of writing the audit information of each business in the content audit to the local storage.

content-audit write-db { url | web-search | web-bbs | web-mail | mail | im | app-control | vid }

Turns off the switch for writing the audit information of each business in the content audit to the local storage.

no content-audit write-db { url | web-search | web-bbs | web-mail | mail | im | app-control | vid }

【Parameter Description】-

【Default Configuration】 ACE product: application control auditing (app-control) is enabled by default, other services are disabled by default; other products: all services are enabled by default.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】When the audit information of each business of the content audit is sent to the external log server, this switch can be turned off, and the database will not be written locally, reducing the burden on the device.

【Configuration Example]】1: Enable the switch of writing url audit information to local storage.

```
AC-FS#  configure  terminal AC-FS(config)#
content-audit write-db url
AC-FS(url-obj-config)# end
```

2: Turn off the switch for writing url audit information to local storage.

```
AC-FS# configure terminal
AC-FS(config)# no content-audit write-db url
AC-FS(url-obj-config)# end
```

【Verification】Use the show content-audit write-db/show running-config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 Products with built-in storage are supported, products without built-in storage are not supported.

16.7 content-audit http-port

Add an HTTP port.

content-audit http-port port-num

Remove an HTTP port.

no content-audit http-port port-num

【Parameter Description】

Parameter	Description
port-num	Port number, range: 1~65535, where 80 and 8080 are in-system ports, not allowed to match place, delete.

【Default Configuration】 None.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】When the application identification is not enabled, when a website needs to be audited, but the port is not 80 or 8080, you can use this command to add the port of this website to the HTTP port, and the website can be audited.

【Configuration Example]】1: Add port 60000 as the HTTP port.

```
AC-FS# configure terminal
AC-FS(config)# content-audit http-port 60000
AC-FS(url-obj-config)# end
```

2: Remove port 60000 from HTTP ports.

```
AC-FS# configure terminal
AC-FS(config)# no content-audit http-port 60000
AC-FS(url-obj-config)# end
```

【Verification】 Use the show content-audit http-port or show running-config command to view the configuration information.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 All gateway series products are supported.

16.8 content-audit https-port

Add an HTTPS port.

content-audit https-port port-num

Remove an HTTPS port.

no content-audit https-port port-num

【Parameter Description】

Parameter	Description
port-num	Port number, range: 1~65535, where 443 is the fixed port in the system, not allowed to configure, delete get rid of.

【Default Configuration】 None.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 When the application identification is not enabled, when an HTTPS encrypted website needs to be audited, but the port is not 443, you can use this command to add the port of this website to the HTTPS port, and the website can be audited.

【Configuration Example]】1: Add port 4430 as the HTTPS port.

```
AC-FS# configure terminal
AC-FS(config)# content-audit https-port 4430
AC-FS(url-obj-config)# end
```

2: Remove port 4430 from HTTP ports.

```
AC-FS# configure terminal
AC-FS(config)# no content-audit https-port 4430
AC-FS(url-obj-config)# end
```

【Verification】Use the show content-audit https-port or show running-config command to view the configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 It is supported by all EG series and NBR series products, but not supported by other series of gateway products.

16.9 content-object

Specify the content object name and enter the content object configuration mode.

content-object object-name

Deletes the content object, and any keywords it contains.

no content-object object-name

【Parameter Description】

Parameter	Description
object-name	Content object name.The maximum length is 40 bytes.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Use this command to configure the content object. The content object capacity is 100.

【Configuration Example]】1: Configure a content object objA, including the keyword hello and the regular match .ietf.org.

```
AC-FS#  configure  terminal AC-FS(config)#
content-object objA AC-FS(content-obj-
config)# keyword hello
AC-FS(content-obj-config)# regexp .*\.ietf\.org
AC-FS(content-obj-config)# end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 MSC does not support, other gateway series products support.

16.10 content-policy

Specify the content audit policy group name and enter the content audit policy group configuration mode.

content-policy policy-name

Delete the content audit policy group, and all the rules it contains.

no content-policy policy-name

【Parameter Description】

Parameter	Description
policy-name	Content Audit Policy group name. The maximum length is 100 bytes.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Use this command to configure policy groups. The policy group has a capacity of 100.

【Configuration Example]】1: Configure a content audit policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 All gateway series products are supported.

16.11 content-policy-config

Globally disable custom policy groups.

content-policy-config disable-all

Cancel the global disable of the custom policy group.

no content-policy-config disable-all

Disable a policy group.

content-policy-config disable-policy policy-name

Un-disable the policy group.

no content-policy-config disable-policy policy-name

Swap the priorities of the two policy groups.

content-policy-config priority-swap policy-name1 policy-name2

【Parameter Description】

Parameter	Description

policy-name	Another policy group name that the priority.
policy-name1	Policy group name requiring a priority adjustment.
policy-name2	Content Audit Policy group name.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 1: Global disable only works for custom policy groups, not for built-in policy groups.

2: The policy group is valid by default. Disabling a policy group provides a way to retain a policy group configuration, but not use the policy group. To disable a policy group, you need to explicitly configure a disable command.

3: Disabling a policy group does not delete the policy group content and association with the user.

4: When configuring the disable policy group command, if the specified policy group name does not exist, the command will not take effect.

5: After the policy group is deleted, the disabled policy group configuration will also be deleted at the same time.

6: After configuring and exchanging the priorities of the two policy groups, you can see that the order of the two policy groups has changed in show running-config, but this command will not appear in show running-config.

【Configuration Example]】 1: Close all custom policy groups.

```
AC-FS# configure terminal
AC-FS(config)# content-policy-config disable-all
AC-FS(config)# end
```

2: Disable the content audit policy group policyA.

```
AC-FS# configure terminal
AC-FS(config)# content-policy-config disable-policy policyA AC-
FS(config)# end
```

3: Exchange the priorities of the two policy groups policyA and policyB.

```
AC-FS# configure terminal
AC-FS(config)# content-policy-config policy-swap policyA policyB AC-FS(config)#
end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 All gateway series products are supported.

16.12 content-policy-relate

Sets the policy that users do not inherit the parent user group.

content-policy-relate no-inherit { subscriber { subs-name1 } | auth-subscriber { subs-name2 | any } }

Restores the user's policy inheritance properties.

no content-policy-relate no-inherit { subscriber { subs-name1 } | auth-subscriber { subs-name2 | any } }

Associate policy groups to users.

content-policy-relate relate { subscriber { subs-name1 } | auth-subscriber { subs-name2 | any } } policy policy-name

Remove the user's association with the policy group. .

no content-policy-relate relate { subscriber { subs-name1 } | auth-subscriber { subs-name2 | any } } policy policy-name

【Parameter Description】

Parameter	Description
subs-name1	Policy group name.
subs-name2	Certified user associated with the policy group.
policy-name	Static users associated with the policy group.The Internet cafe version of NBR products can also be associated with custom user groups.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】1: When configuring the user's policy inheritance attribute, the specified user subs-name1 and subs-name2 may not exist. If there is a policy association at this time, the command can exist, but the rule does not take effect. When a user is removed from all policy groups, the user's Disable Policy Inheritance property is also removed.

2: When configuring an association rule, if the policy group name does not exist, the association operation will not take effect and the command will not exist.

3: When configuring an association rule, the associated users subs-name1 and subs-name2 may not exist. At this time, the command can exist, but the rule does not take effect.

4: When configuring association rules, subscriber or auth-subscriber can specify multiple user names, separated by commas, indicating that multiple users are associated with the policy group. policy-name also allows specifying multiple policy groups, separated by commas.

【Configuration Example]】1: Configure static user user1 not to inherit the policy of its parent user group.

```
AC-FS# configure terminal
AC-FS(config)# content-policy-relate no-inherit subscriber user1 AC-FS(config)#
end
```

2: Configure a content audit policy group named policyA to associate with the static users user1 and user2, and also associate policyA and policyB with the authentication user auth-user3. Configure a policy group named policyC associated with the custom user group cstm_grp1.

```
AC-FS# configure terminal
AC-FS(config)# content-policy-relate relate subscriber usr1,user2 policy policyA AC-FS(config)#
content-policy-relate relate auth-subscriber auth-user3 policy policyA,policyB AC-FS(config)#
content-policy-relate relate subscriber cstm_grp1 policy policyC AC-FS(config)# end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 All gateway series products are supported.

16.13im-rule

Enable IM default auditing.

im-rule audit-default-enable

Disable the default audit function of IM.

no im-rule audit-default-enable

Delete all IM rules under the policy group.

im-rule delete-all

Exchange the priority of IM access control rules.

im-rule priority-swap rule-id1 rule-id2

Add the public section of IM access control rules to the content audit policy group.

im-rule rule-id time-range time-name action { permit | deny } [audit] [comment comment-string]

Add a further ParameterDescription of the IM access control rule to the content audit policy group, mainly the keyword matching conditions of the Description rule. This command must be used in conjunction with the im-rule rule-id time-range command.

im-rule rule-id im-type im-name [relation { and | or } [account content-object-name1] [message

content-object-name2]]

Delete IM access control rules.

no im-rule rule-id

【Parameter Description】

Parameter	Description
rule-id1	Chat record, missing item indicates that the item does not match.
rule-id2	IM account, missing this item means that it does not have to match it.
rule-id	Indicates the IM software for the audit.The im-name represents a specific string string.For example, the string string is "qq" means that this rule only audits the QQ software; the string string is "qq, msn" or"
time-name	The msn, qq " indicates that this rule audits only the QQ software and the MSN software.
comment-string	The Description of the rule.
im-name	Time object name representing the time period when the rule takes effect.
content-object-name1	ID identification of the rule, value range (1~200), and a rule capacity of 200.

content-object-name2	The ID of Rule 2 for the priority level to be exchanged.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Content audit policy group configuration mode

【Default Level】 14

【Usage Guide】 1: The rule-id of a rule is not allowed to be repeated in the same content audit policy group, but is allowed to be repeated in different content audit policy groups.

2: The access control rules in a content audit policy group have corresponding priorities, and the rule assigned last has the highest priority.

3: The time-name and content-object-name associated with the rule may not exist, and the rule will not take effect at this time.

4: QQ chat is encrypted information and currently does not support content filtering and auditing (if im-name is QQ, message cannot be configured).

5: The swap priority command is used to swap the priorities of two access control rules. After running this command, you can see that the order of the two rules has changed in show running-config, but the order of the two rules will not appear in show running-config. Order.

6: The default audit can only be configured in the default audit group whose policy group name is _AUDIT_DEFAULT, and this command will not take effect if configured in other policy groups.

【Configuration Example]】 1: Enable IM default auditing.

```
AC-FS# configure terminal
AC-FS(config)# content-policy _AUDIT_DEFAULT
AC-FS(cont-plcy-config)# im-rule audit-default-enable
AC-FS(cont-plcy-config)# end
```

2: Delete all IM rules in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# im-rule delete-all
AC-FS(cont-plcy-config)# end
```

3: Exchange the priority of IM access control rule 10 and rule 20 in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# im-rule priority-swap 10 20
AC-FS(cont-plcy-config)# end
```

4: Add an MSN access audit rule to the content audit policy group policyA, which allows users to conduct MSN chat, and needs to audit the user's specific account accountA or specific chat keyword keyA information.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# im-rule 2 time-range any action permit audit comment PermitUserAMSN
AC-FS(cont-plcy-config)# im-rule 2 im-type msn relation or account accountA message keyA
AC-FS(cont-plcy-config)# end
```

【Verification】 Use the show running-config command to view the configuration status.

【Prompt Information】 1: If the configured rule-id already exists, a prompt will be given.

```
AC-FS(config)# im-rule 2 time-range any action permit audit comment PermitUserAMSN
Rule 2 already exists, please delete it first
```

2: If the public part of the rule is not configured, and the further Description of the rule is directly configured, a prompt will be given.

```
AC-FS(config)# im-rule 2 im-type msn relation or account accountA message keyA
Rule 2 is not exist
```

【Common Mistake】 -

【Platform Description】 MSC products do not support, other gateway series products are supported.

16.14keyword

Add keywords to content objects.

keyword string

Delete keywords.

no keyword string

【Parameter Description】

Parameter	Description
string	Keywords that the content object contains. The maximum length is 100 bytes.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Content object configuration mode

【Default Level】 14

【Usage Guide】 Use this command to configure the keywords contained in the content object.

【Configuration Example]】1: Configure a content object objA containing the keyword hello.

```
AC-FS#  configure  terminal AC-FS(config)#
content-object objA AC-FS(content-obj-
config)# keyword hello
AC-FS(content-obj-config)# end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 MSC products do not support, other gateway series products are supported.

16.15mail-rule

Enable MAIL default auditing.

mail-rule audit-default-enable

Disable the default audit function of MAIL.

no mail-rule audit-default-enable

Delete all MAIL rules under the policy group.

mail-rule delete-all

Exchange the priority of MAIL access control rules.

mail-rule priority-swap rule-id1 rule-id2

Add the public section of the MAIL access control rule to the content audit policy group.

mail-rule rule-id time-range time-name [direction { in | out | double }] action { permit | deny } [audit] [comment comment-string]

Add a further ParameterDescription of the MAIL access control rule to the content audit policy group, mainly the keyword matching conditions of the Description rule. This command is optional. If it is not configured, it means to audit all mail information that meets the mail-rule rule-id time-range command.

mail-rule rule-id relation { and | or } [from content-object-name1] [to content-object-name2] [subject content-object-name3] [body content-object-name4] [attachment-name content- object-name5] [mail-size { greater | greater-equal | less | less-equal } file-size]

Delete the MAIL access control rule.

no mail-rule rule-id

【Parameter Description】

Parameter	Description
rule-id1	File size value, as an integer, in Kbytes.
rule-id2	Attachment name keyword, missing item does not match.
rule-id	Message content keyword, missing item indicates that it does not match.
time-name	Message title keyword, missing item indicates that it does not match.
comment-string	Recipient keyword, missing item does not match the item.
content-object-name1	Sender keyword, missing item means not match.
content-object-name2	The Description of the rule.
content-object-name3	Time object name representing the time period when the rule takes effect.
content-object-name4	ID identification of the rule, value range (1~200), and a rule capacity of 200.
content-object-name5	The ID of Rule 2 where the priority is to be exchanged.
file-size	The ID of Rule 1 where the priority is to be exchanged.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Content audit policy group configuration mode

【Default Level】 14

【Usage Guide】 1: The rule-id of a rule is not allowed to be repeated in the same content audit policy group, but is allowed to be repeated in different content audit policy groups.

2: The access control rules in a content audit policy group have corresponding priorities, and the rule assigned last has the highest priority.

3: The time-name and content-object-name associated with the rule may not exist, and the rule will not take effect at this time.

4: When the rule is configured as blocking, only the or relation in relation will be valid.

5: The swap priority command is used to swap the priorities of two access control rules. After running this command, you can see that the order of the two rules has changed in show running-config, but the order of the two rules will not appear in show running-config. Order.

6: The default audit can only be configured in the default audit group whose policy group name is _AUDIT_DEFAULT, and this command will not take effect if configured in other policy groups.

【Configuration Example]】 1: Enable MAIL default auditing.

```
AC-FS# configure terminal
AC-FS(config)# content-policy _AUDIT_DEFAULT AC-FS(cont-
plcy-config)# mail-rule audit-default-enable AC-FS(cont-
plcy-config)# end
```

2: Delete all MAIL rules in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# mail-rule delete-all
AC-FS(cont-plcy-config)# end
```

3: Exchange the priority of MAIL access control rule 10 and rule 20 in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# mail-rule priority-swap 10 20
AC-FS(cont-plcy-config)# end
```

4: Add a MAIL access control rule to the content audit policy group policyA to allow all users to send emails, and audit emails whose sender matches the OBJ-F keyword, or whose subject matches the OBJ-S keyword, or whose email size is less than 20000Kb.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# mail-rule 1 time-range any action permit audit comment mail-audit-1 AC-
FS(cont-plcy-config)# mail-rule 1 relation or from OBJ-F subject OBJ-S mail-size less 20000
AC-FS(cont-plcy-config)# end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】1: If the configured rule-id already exists, a prompt will be given.

```
AC-FS(config)# mail-rule 1 time-range any action permit audit comment mail-audit-1
Rule 1 already exists, please delete it first
```

2: If the public part of the rule is not configured, and the further Description of the rule is directly configured, a prompt will be given.

```
AC-FS(config)# mail-rule 1 relation or from OBJ-F subject OBJ-S mail-size less 20000
Rule 1 is not exist
```

【Common Mistake】-

【Platform Description】 ACE series products do not support, other products with built-in storage support; NBR-E series, EG2000F products support, other products without built-in storage are not supported.

16.16 Regexp

Add a URL regular expression to the URL object.

regexp url-regexp

Remove URL regular expressions.

no regexp url-regexp

Add a keyword regular expression to the content object.

regexp regexp

Remove keyword regular expressions.

no regexp regexp

【Parameter Description】

Parameter	Description
url-regexp	Keyword regular expression that supports the standard regular notation.
regexp	URL regular expression, supporting the standard canonical notation.

【Default Configuration】 There is no configuration by default.

【Command Mode】 URL object configuration mode, content object configuration mode

【Default Level】 14

【Usage Guide】 Use this command to configure the regular expression contained in the URL object or content object.

【Configuration Example]】 1: Add a regular expression to the URL object url-objA to match URLs that contain the ieft keyword.

```
AC-FS# configure terminal
AC-FS(config)# url-object url-objA AC-
FS(url-obj-config)# regexp .*ieft.*
AC-FS(url-obj-config)# end
```

2: Configure a content object objA containing the keyword hello and the regular match .ietf.org.

```
AC-FS#  configure  terminal AC-FS(config)#
content-object objA AC-FS(content-obj-
config)# keyword hello
AC-FS(content-obj-config)# regexp .*\.ietf\.org
AC-FS(content-obj-config)# end
```

【Verification】 Use the show running-config command to view the configuration status.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 All gateway series products are supported.

16.17 show app-audit detail

Query the detailed information of the application control audit.

show app-audit detail [export] { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name1] [auth-subscriber subs-name2] [app-group app-group-name] [rule-name rule-name] [ip addr] [permit | deny] order-by { time | subscriber | internal-ip | app } { asc | desc } [start-item integer1 end-item integer2]

【Parameter Description】

Parameter	Description
hours	Filter condition: Certified user name, exact match.
yyyy mm dd	Filter condition: static user name, exact matching.
hh:mm:ss	Bridge number.
hour1	Interface name.
hour2	Time period filter conditions: End of the hour period.
hour3	Time period filter condition: start hour period.
hour4	Time period filter conditions: End of the hour period.
intf-name	Time period filter condition: start hour period.
bridge-num	Hour minutes seconds.
subs-name1	YTD.
subs-name2	Recent time period.
app-group-name	End location in the query results collection.
rule-name	Start location in the query results set.
addr	Filter conditions: IP, exact match; multiple IP are separated by ",".
integer1	Filter criteria: The matched rule name.
integer2	Filter condition: Application group name.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query or export the detailed information of application control audit.

【Configuration Example]】 1: Query the application control audit details of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

```
AC-FS# show app-audit detail time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
order-by time desc start-item 1 end-item 20
==========================================================================
Time: 2013-05-03 16:45:29
subscriber: /userA
auth-subscriber: any
Ip: 192.168.211.96
App:  QQ
Rule: DenyQQ
Action: deny
.....
```

【Prompt Information】-

【Platform Description】 Products with built-in storage are supported, products without built-in storage are not supported.

16.18 show app-audit stat

Query application control audit statistics.

show app-audit stat { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name1] [auth-subscriber subs-name2] [ip addr] [app-group app-group-name] [rule-name rule- name] [permit | deny]

【Parameter Description】

Parameter	Description
hours	Filter criteria: The matched rule name.
yyyy mm dd	Filter condition: Application group name.
hh:mm:ss	Filter conditions: IP, exact match; multiple IP are separated by ",".
hour1	Filter condition: Certified user name, exact match.
hour2	Filter condition: static user name, exact matching.
hour3	Bridge number.
hour4	Interface name.
intf-name	Time period filter conditions: End of the hour period.
bridge-num	Time period filter condition: start hour period.

subs-name1	Time period filter conditions: End of the hour period.
subs-name2	Time period filter condition: start hour period.
addr	Hour minutes seconds.
app-group-name	YTD.
rule-name	Recent time period.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query the statistics of application control audit.

【Configuration Example]】1: Query the application control audit statistics of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

```
AC-FS# show app-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
50
```

【Prompt Information】-

【Platform Description】 Products with built-in storage are supported, products without built-in storage are not supported.

16.19 show content-audit statistics

Displays real-time statistics for content auditing.

show content-audit statistics { brief | counts }

【Parameter Description】

Parameter	Description
brief	Displays count information for real-time content audit statistics, including total and blocking records.
stat	Display a summary of real-time content audit statistics, showing only the last 50 records.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to view the summary information or count information of real-time statistics.

【Configuration Example]】 1: View the summary information of real-time statistics.

```
AC-FS#show content-audit statistics brief

audit-totle-number:3

    id      relate-user       audit-time           action  key-type
_________  ________________  ___________________  ______  ____________________________

         3  220.181.12.101    2014-02-10 00:02:50  permit  recv-mail-title:
         2  113.108.16.116    2014-02-09 14:26:31  permit  recv-mail-title: : hello

         1  192.168.66.111    2014-02-09 14:26:08  permit  send-mail-title: : hello
```

2: View the counting information of real-time statistics.

```
AC-FS#show content-audit statistics counts


start-time: 2014-02-09 14:25:22


application control information:

    totle-num: 0

    block-num: 0


url reference host:

    totle-num: 0

    block-num: 0


web-search keyword:

    totle-num: 0

    block-num: 0


web-bbs post information:
```

```
    totle-num: 0
    block-num: 0

web-mail information:
    totle-num: 0
    block-num: 0

MSN information:
    totle-num: 0
    block-num: 0

QQ information:
    totle-num: 0
    block-num: 0

POP3 mail information:
    totle-num: 2
    block-num: 0

SMTP mail information:
    totle-num: 1
    block-num: 0
```

【Prompt Information】-

【Platform Description】 All gateway series products are supported.

16.20 show content-audit write-db

Displays the toggle status of whether the content audit audit writes to local storage.

show content-audit write-db

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to check whether the audit information of each business of the content audit is written to the local storage switch status.

【Configuration Example]】1: View the on/off status of writing to local storage for each business of content auditing.

```
AC-FS#show content-audit write-db
url_write_db:           1
web_search_write_db: 1
web_bbs_write_db:       1
web_mail_write_db:      1
mail_write_db:          1
im_write_db:            1
app_control_write_db:   1
```

【Prompt Information】-

【Platform Description】 Products with built-in storage are supported, products without built-in storage are not supported.

16.21 show content-audit http-port

Display HTTP port information.

show content-audit http-port

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to view HTTP port information.

【Configuration Example]】1: View HTTP port information.

```
AC-FS#show content-audit http-port
```

```
HTTP port information in user:       80  8080 60000
HTTP port information in kernel:     80  8080 60000
```

【Prompt Information】-

【Platform Description】 All gateway series products are supported.

16.22 show content-audit https-port

Display HTTPS port information.

show content-audit https-port

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to view HTTPS port information.

【Configuration Example]】1: View HTTPS port information.

```
AC-FS#show content-audit https-port
HTTPS port information in user:     443 4430
HTTPS port information in kernel:  443  4430
```

【Prompt Information】-

【Platform Description】 It is supported by all EG series and NBR series products, but not supported by other series of gateway products.

16.23 show content-policy

【Parameter Description】

Parameter	Description

content-policy	Displays all the policy details within the specified policy group.
policy	The command ends directly with the Parameter, showing all policy groups and all policies within the group.
stat	Policy Group Name.Specifies that the Parameter represents a policy policy within the query named policy-name .
all-rule	A little information.
policy-name	Show all policy groups and all policy details in policy groups.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query policy group related information.

【Configuration Example]】 1: View all existing policy groups and the overview of all policies in the group.

```
AC-FS#show content-policy
content-policy _TOP_PRIORITY
(active)app-rule 200 time-range any app-group Block_Group action deny audit
(active)app-rule 197 time-range any app-group Block_Group action deny audit vpn

content-policy _AUDIT_DEFAULT
(active)url-rule audit-default-enable
(active)im-rule audit-default-enable
```

2: View the details of the specified policy group and all policies in the group

```
AC-FS#show content-policy policy _AUDIT_DEFAULT
policy-type: url-rule

rule-id         :0
unit-id         :0
url-object      :any
rule->obj_id  :0
action          :permit
audit           :Y time-
range      :
effective       :1
comment         :default_audit
```

```
_____________________________________________

policy-type: im-rule

rule-id : 0 time-
range  :
rule-type  : msn,qq
keyword           :
action          : permit
audit           : Y
effective  : 1
comment         : default_audit
```

3: Check the status of the custom policy group (whether the policy group exists and how many ids).

```
AC-FS#show content-policy stat _AUDIT_DEFAULT
exist: yes
policy_id:1
```

4: Details of all policy groups and all policies in the group.

```
AC-FS#show content-policy all-rule
content-policy _TOP_PRIORITY
policy-type: app-rule

rule-id         : 197
unit-id         : 2
app-name        : Block_Group
app-id          : 4294967279
action          : deny
audit           : Y
vpn             : Y
vip             : N
```

```
time-range      : any
effective       : 1
comment         :

rule-id         : 200
unit-id         : 1
app-name        : Block_Group
app-id          : 4294967279
action          : deny
audit           : Y
vpn             : N
vip             : N
time-range      : any
effective       : 1
comment         :

----------------------------------------------------------------------------------------------------

content-policy _AUDIT_DEFAULT
policy-type: url-rule

rule-id         :0
unit-id         :0
url-object      :any
rule->obj_id  :0
action          :permit
audit           :Y time-
range      :
effective       :1
comment         :default_audit

----------------------------------------------------------------------------------------------------
```

```
policy-type: im-rule


rule-id : 0 time-

range  :

rule-type  : msn, qq

keyword          :

action          : permit

audit           : Y

effective  : 1

comment         : default_audit


_____
```

【Prompt Information】-

【Platform Description】 All gateway series products are supported.

16.24 show content-policy-relate

Displays user and policy association information in a policy view.

show content-policy-relate policy-view [{ policy policy-name | { subscriber { subs-name1 } |

auth-subscriber { subs-name2 } }]

Displays user and policy association information in a user view.

show content-policy-relate user-view { subscriber { subs-name1 } | auth-subscriber { subs-name2 } } [detail]

【Parameter Description】

Parameter	Description
policy-name	IP, address.
subs-name1	Certified username.
subs-name2	Static user name.
A.B.C.D	Policy name or a custom user group name.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query the user information associated with the policy, or query the policy information associated with the user.

【Configuration Example]】 1: View the association information of the static user name userA in the policy view.

```
AC-FS#show content-policy-relate policy-view subscriber userA
policy-name: policyA
disable: off
pri: 1
effective: 1 (1/1/1)
subscriber: userB userA
auth-subscriber:
```

2: View the associated information of the static user name userA in the user view.

```
AC-FS#show content-policy-relate user-view subscriber userA
policy-name: policyA
pri: 1
disable: on
effective: 1 (1/1/1)
relation-disable: on
inherit: 0
------------------------------------------------

policy-summary: 1/0
user-inherit: 1
```

3: View the association information of the user whose IP address is A.B.C.D in the policy view (this IP is added to the custom user group cstm_grp1).

```
AC-FS#show content-policy-relate policy-view ip A.B.C.D
policy-name: policyC
disable: off
pri: 3
effective: 1 (1/1/1)
subscriber: cstm_grp1
auth-subscriber:
```

4: View the associated information of the user whose IP address is A.B.C.D in the user view.

```
AC-FS#show content-policy-relate user-view ip A.B.C.D
policy-name: policyC
pri: 3
disable: on
effective: 1 (1/1/1)
relation-disable: on
inherit: 0
————————————————————————————————

policy-summary: 1/0
user-inherit: 1
```

【Prompt Information】 -

【Platform Description】 All gateway series products are supported.

16.25show im-audit detail

Query the detailed information of IM audit.

show im-audit detail [export] { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name1] [auth-subscriber subs-name2] [direction { in | out | double }] [type { qq | msn }] [message keyword] [account account-string] [rule-name rule-name] [ip addr] [permit | deny] order-by { time | subscriber | auth-subscriber | internal-ip | direction } { asc | desc } [start-item integer1 end-item integer2]

【Parameter Description】

Parameter	Description
hours	recent time period.
yyyy mm dd	year month day.
hh:mm:ss	hours minutes seconds.
hour1	Time period filter: Start hour period.
hour2	Period Filter: End Hours.
hour3	Time period filter: Start hour period.
hour4	Period Filter: End Hours.
intf-name	interface name.
bridge-num	bridge number.
subs-name1	Filter condition: static username, exact match.
subs-name2	Filter Condition: Authentication Username, Exact Match.
keyword	Filter by: Chat History.
account-string	Filter by: Chat Account.
rule-name	Filter Condition: Matched Rule Name.
addr	Filter conditions: IP, exact match; multiple IPs are separated by ",".
integer1	The starting position in the query result set.
integer2	The end position in the query result set.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query or export the detailed information of IM audit.

【Configuration Example]】1: Query the MSN audit details of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

```
AC-FS# show im-audit detail time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
type msn order-by time desc start-item 1 end-item 20
================================================================================================

Time: 2013-05-03 15:45:59

App-type: msn

Sender: userA@hotmail.com

Receiver: userB@yahoo.com

Direction: out

Path: GigabitEthernet 0/5

Ip: 192.168.211.96

User: /userA Auth-

User: Match-Rule:

ruleA Action:

permit Message:

hello!

------
```

【Prompt Information】-

【Platform Description】 Products with built-in storage are supported, products without built-in storage are not supported.

16.26 show im-audit stat

Query the statistics of IM auditing.

show im-audit stat { recent hours | time-range from yyyy mm dd hh:mm::ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name1] [auth-subscriber subs-name2] [direction { in | out | double }] [type { qq | msn }] [message keyword] [account account-string] [rule-name rule-name] [ip addr] [permit | deny]

【Parameter Description】

Parameter	Description
hours	recent time period.
yyyy mm dd	year month day.
hh:mm:ss	hours minutes seconds.
hour1	Time period filter: Start hour period.

hour2	Period Filter: End Hours.
hour3	Time period filter: Start hour period.
hour4	Period Filter: End Hours.
intf-name	interface name.
bridge-num	bridge number.
subs-name1	Filter condition: static username, exact match.
subs-name2	Filter Condition: Authentication Username, Exact Match.
keyword	Filter by: Chat History.
account-string	Filter by: Chat Account.
rule-name	Filter Condition: Matched Rule Name.
addr	Filter condition: intranet ip.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query the statistics of IM audit.

【Configuration Example]】1: Query the MSN audit statistics of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

```
AC-FS# show im-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA type
msn
50
```

【Prompt Information】-

【Platform Description】 Products with built-in storage are supported, products without built-in storage are not supported.

16.27 show mail-audit attachment-info

Query the attachment information of an email.

show mail-audit attachment-info timestamp timestamp rand-id rand-id

【Parameter Description】

Parameter	Description

timestamp	stochastic,id.
rand-id	time stamp.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 First use the command show mail-audit detail to view the timestamp and random id of the email, and then use this command to query the attachment information of a certain email.

【Configuration Example]】1: Query the attachment information of the email whose timestamp is 1286849291 and rand-id is 1087821567.

```
AC-FS#show mail-audit attachment-info timestamp 1286849291 rand-id 1087821567
Size(Byte)  Path
============================================================
80646       mnt/sata/mail/20130503/unknown(09-01-19-44-40).gif
150528      mnt/sata/mail/20130503/test-file.doc
```

【Prompt Information】-

【Platform Description】 ACE series products do not support, other products with built-in storage support, all devices without built-in storage are not supported.

16.28show mail-audit detail

Query the detailed information of the MAIL audit.

show mail-audit detail [export] { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name1] [auth-subscriber subs-name2] [ip addr] [direction { in | out | double }] [from keyword1] [to keyword2] [subject keyword3] [rule-name rule-name] [permit | deny] order-by { time | subscriber | auth-subscriber | internal-ip | direction | send-mail-addr | mail-size } { asc | desc } [start-item integer1 end-item integer2]

【Parameter Description】

Parameter	Description
hours	recent time period.
yyyy mm dd	year month day.

hh:mm:ss	hours minutes seconds.
hour1	Time period filter: Start hour period.
hour2	Period Filter: End Hours.
hour3	Time period filter: Start hour period.
hour4	Period Filter: End Hours.
intf-name	interface name.
bridge-num	bridge number.
subs-name1	Filter condition: static username, exact match.
subs-name2	Filter Condition: Authentication Username, Exact Match.
addr	Filter conditions: IP, exact match; multiple IPs are separated by ",".
keyword1	Filter by: Email sender keyword.
keyword2	Filter by: Email recipient keywords.
keyword3	Filter condition: Email subject keyword.
rule-name	Filter Condition: Matched Rule Name.
integer1	The starting position in the query result set.
integer2	The end position in the query result set.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query or export the detailed information of MAIL audit.

【Configuration Example]】1: Query the MAIL audit details of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

```
AC-FS# show mail-audit detail time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
order-by time desc start-item 1 end-item 20
=============================================================================================
Time: 2013-05-03 15:45:59
App-type: SMTP
Direction: out
Path: GigabitEthernet 0/5
Ip: 192.168.211.96
User: /userA Auth-
User: Match-Rule:
ruleA
Action: permit
```

```
Timestamp: 1287027112
Rand-id: 1686175891
From: userA@hotmail.com
To: userB@yahoo.com
Subject: hello
Body: hello
......
```

【Prompt Information】-

【Platform Description】 ACE series products are not supported, other products with built-in storage are supported, and all products without built-in storage are not supported.

16.29 show mail-audit stat

Query the statistics of MAIL audit.

show mail-audit stat { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name1] [auth-subscriber subs-name2] [ip addr] [direction { in | out | double }] [from keyword1] [to keyword2] [subject keyword3] [rule-name rule-name] [permit | deny]

【Parameter Description】

Parameter	Description
hours	recent time period.
yyyy mm dd	year month day.
hh:mm:ss	hours minutes seconds.
hour1	Time period filter: Start hour period.
hour2	Period Filter: End Hours.
hour3	Time period filter: Start hour period.
hour4	Period Filter: End Hours.
intf-name	interface name.
bridge-num	bridge number.
subs-name1	Filter condition: static username, exact match.
subs-name2	Filter Condition: Authentication Username, Exact Match.
addr	Filter conditions: IP, exact match; multiple IPs are separated by ",".
keyword1	Filter by: Email sender keyword.
keyword2	Filter by: Email recipient keywords.
keyword3	Filter condition: Email subject keyword.
rule-name	Filter Condition: Matched Rule Name.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query the statistics of MAIL audit.

【Configuration Example]】1: Query the MAIL audit statistics of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

```
AC-FS# show mail-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
50
```

【Prompt Information】-

【Platform Description】 ACE series products are not supported, other products with built-in storage are supported, and all products without built-in storage are not supported.

16.30show url-audit detail

Query URL audit details.

show url-audit detail [export] { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name] [auth-subscriber auth-subs-name] [ip addr] [url-class class-name | url-object obj-name | url url-string | url-host host-string1] [host host-string2] [permit | deny] [order-by time | url-class | url | host | ip] { asc | desc } [start -item integer1 end-item integer2]

【Parameter Description】

Parameter	Description
hours	recent time period.
yyyy mm dd	year month day.
hh:mm:ss	hours minutes seconds.
hour1	Time period filter: Start hour period.
hour2	Period Filter: End Hours.
hour3	Time period filter: Start hour period.
hour4	Period Filter: End Hours.
intf-name	interface name.
bridge-num	bridge number.
subs-name1	Filter condition: static username, exact match.
subs-name2	Filter Condition: Authentication Username, Exact Match.
addr	Filter conditions: IP, exact match; multiple IPs are separated by ",".
class-name	Filter Condition: URL Category Name, Exact Match.
obj-name	Filter condition: URL object name, exact match.
url-string	Filter: URL String, Fuzzy Match.
host-string1	Filter condition: HOST string, exact match.
host-string2	Filter by: HOST site, exact match.
integer1	The starting position in the query result set.
integer2	The end position in the query result set.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query or export the detailed information of URL auditing.

【Configuration Example]】1: Query the URL audit details of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

【Prompt Information】-

【Platform Description】 It is supported by gateway products with built-in storage, but not supported by gateway products without built-in storage.

```
AC-FS# show url-audit detail time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
order-by time desc start-item 1 end-item 20
=============================================================================================
Time: 2013-05-03 15:45:59
Ip: 192.168.211.96
Subscriber: /userA
Auth-subscriber:
Match-rule: ruleA
Action: permit
URL: http://www.ietf.org/
......
```

16.31 show url-audit stat

Query URL auditing statistics.

show url-audit stat { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name] [auth-subscriber auth-subs-name] [ip addr] [url-class class-name | url-object obj-name] [host host-string] [permit | deny]

【Parameter Description】

Parameter	Description
hours	recent time period.
yyyy mm dd	year month day.
hh:mm:ss	hours minutes seconds.
hour1	Time period filter: Start hour period.
hour2	Period Filter: End Hours.
hour3	Time period filter: Start hour period.
hour4	Period Filter: End Hours.
intf-name	interface name.
bridge-num	bridge number.

subs-name1	Filter condition: static username, exact match.
subs-name2	Filter Condition: Authentication Username, Exact Match.
addr	Filter conditions: IP, exact match; multiple IPs are separated by ",".
class-name	Filter Condition: URL Category Name, Exact Match.
obj-name	Filter condition: URL object name, exact match.
host-string	Filter by: HOST site, exact match.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query the statistics of URL auditing.

【Configuration Example]】1: Query the URL audit statistics of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

```
AC-FS# show url-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
500
```

【Prompt Information】-

【Platform Description】 It is supported by gateway products with built-in storage, but not supported by gateway products without built-in storage.

16.32 show url-audit top

Query URL site access ranking TOPN.

show url-audit top n [export] { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name] [auth-subscriber auth-subs-name] [url-class class-name | url-object obj-name] [host host-string] [permit | deny] [order-by time | url-class | url | url-class | host-times]

【Parameter Description】

Parameter	Description
n	Number of Top n (1~100).
hours	recent time period.
yyyy mm dd	year month day.

hh:mm:ss	hours minutes seconds.
hour1	Time period filter: Start hour period.
hour2	Period Filter: End Hours.
hour3	Time period filter: Start hour period.
hour4	Period Filter: End Hours.
intf-name	interface name.
bridge-num	bridge number.
subs-name1	Filter condition: static username, exact match.
subs-name2	Filter Condition: Authentication Username, Exact Match.
addr	Filter conditions: IP, exact match; multiple IPs are separated by ",".
class-name	Filter Condition: URL Category Name, Exact Match.
obj-name	Filter condition: URL object name, exact match.
host-string	Filter by: HOST site, exact match.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query or export URL site access ranking TOPN.

【Configuration Example]】1: Query the TOP2 site access ranking within 24 hours

```
AC-FS# show url-audit top 2 recent 24
HOST                 Times       url-class          url-object
============================================================
www.ietf.org            32349             class1         obj1
www.w3c.org             30032             class2         obj2
```

【Prompt Information】-

【Platform Description】 It is supported by gateway products with built-in storage, but not supported by gateway products without built-in storage.

16.33 show url-class system

Displays the category names of the current URL library of the system.

show url-class system [class { id class-id | name class-name }]

Displays the description information of the current URL library of the system.

show url-class system comment [class { id class-id | name class-name }]

Displays current custom modification information for the system URL library.

show url-class system custom [class { id class-id | name class-name }]

Displays information about the precise filter library.

show url-class system exact

【Parameter Description】

Parameter	Description
class-name	View information for the specified system taxonomic name class-name; not specified class means viewing all systems. Unified URL classification information
class-id	View the information for the specified system classification ID class-id.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query information about the system URL library.

【Configuration Example]】1: View the category names of the current URL library of the system.

```
AC-FS# show url-class system version-1.0
2010-4-22

system-url-class-number:32
broad heading 1
Job recruitment
IT class
WEB communication
violence
Viral category 2
science
grow up
(omitted below)
```

2: View the current URL library grouping and classification information of the system.

```
AC-FS# show url-class system custom

version-1.0 2010-4-22
system-url-class-number:32 consumption-amount:2
remain-amount:998 (These lines are some necessary statistics.)
broad heading 1
        url-class: Job recruitment

          comment: Job
          recruitmentDescription

                add: add2.com

                move: move1.com

                move: move2.com
        url-class:  military affairs
              comment: Military
classDescription
        url-class:IT class

            comment: IT
            classDescription

                add: add2.com

                move: move1.com

                move: move2.com
  broad heading 2      url-class:

                comment:

          (omitted below)
```

3: View the current URL library classification and Description information of the system.

```
AC-FS# show url-class system comment version-1.0
2010-4-22
```

```
System url class number:32
broad heading 1
Job Recruitment: Description Information 1
Class IT: Description Information 2
WEB communication: Description Information 3
……()
```

4: View the relevant information of the precise filter library

```
AC-FS# show url-class system exact

exact-filter: disable
```

【Prompt Information】-

【Platform Description】 All gateway series products are supported.

16.34 show url-class url

Displays the system url category to which the specified url-string belongs and the actual url category under the current configuration.

show url-class url url-string

【Parameter Description】

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query the system url category to which the specified url-string belongs and the actual url category under the current configuration.

【Configuration Example]】1: Display the category information whose URL is AC-FS.com.cn.

Parameter	Description
url-string	String representing the url.

【Prompt Information】-

【Platform Description】 All gateway series products are supported.

16.35 show url-class user-cfg

Displays configuration information for custom URL categories.

show url-class user-cfg [class-name]

【Parameter Description

Parameter	Description
class-name	Custom classification name

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query the configuration information of the custom URL category.

【Configuration Example]】1: Display the configuration information of each custom URL category.

```
AC-FS# show url-class user-cfg
url-class:CLASSA
url:ietf.org
comment:comment for CLASSA
url-class:CLASSB
url:w3c.org
comment:comment for CLASSB
```

2: Display the configuration information of the specified URL category.

```
AC-FS# show url-class user-cfg CLASSA
url-class:CLASSA
url:ietf.org
comment:comment for CLASSA
```

【Prompt Information】-

【Platform Description】 All gateway series products are supported.

16.36 show web-bbs-audit detail

Query the detailed information of WEB-BBS audit.

show web-bbs-audit detail [export] { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name1] [auth-subscriber subs-name2] [ip addr] [content keyword] [rule-name rule-name] [permit | deny] order-by { time |

subscriber | auth-subscriber | internal-ip | url } { asc | desc } [start-item integer1 end-item integer2]

【Parameter Description】

Parameter	Description
hours	recent time period.
yyyy mm dd	year month day.
hh:mm:ss	hours minutes seconds.
hour1	Time period filter: Start hour period.
hour2	Period Filter: End Hours.
hour3	Time period filter: Start hour period.
hour4	Period Filter: End Hours.
intf-name	interface name.
bridge-num	bridge number.
subs-name1	Filter condition: static username, exact match.
subs-name2	Filter Condition: Authentication Username, Exact Match.
addr	Filter conditions: IP, exact match; multiple IPs are separated by ",".
keyword	Filter conditions: filter keywords, support multi-keyword filtering, separate keywords with commas.
rule-name	Filtering condition: Matching rule name, support multiple rule name filtering, different rule names are separated by half-width commas.
integer1	The starting position in the query result set.
integer2	The end position in the query result set.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query or export the detailed information of WEB-BBS audit.

【Configuration Example]】1: Query the WEB-BBS audit details from 0:00 on 2016-9-4 to 24:00 on 2016--11-4.

```
AC-FS# show web-bbs-audit detail time-range from 2016 9 4 0:0:0 to 2016 11 4 23:59:59 subscriber
userA order-by time desc start-item 1 end-item 20
================================================================
```

```
id: 8
attach_id:
time_stamp: 1480323032
day_time: 2016-11-28 16:50:32
sip: 3.3.3.54
dip: 101.71.8.134
sport: 58439
dport: 80
mac_addr: f48e.388f.f50d
usr_grp: /
usr_name: 3.3.3.54
plcy_name: _AUDIT_DEFAULT
rule_name: default_audit
obj_name:
action: permit
username: lixia_mail@163.com
nickname: sglzooo
uid:
app_type: 网易博客发帖
url: /sglzooo/editBlogNew.do?p=1&n=1&from=bloglist
subject: 2016.11.28.....
```

【Prompt Information】-

【Platform Description】 ACE series products do not support, other gateway products with built-in storage support; all gateway products without built-in storage are not supported.

16.37 show web-bbs-audit stat

Query WEB-BBS audit statistics.

show web-bbs-audit stat { recent hours | time-range from yyyy mm dd hh:mm::ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name1] [auth-subscriber subs-name2] [ip addr] [content keyword] [rule-name rule-name] [permit | deny]

【Parameter Description】

Parameter	Description
hours	recent time period.
yyyy mm dd	year month day.
hh:mm:ss	hours minutes seconds.
hour1	Time period filter: Start hour period.
hour2	Period Filter: End Hours.
hour3	Time period filter: Start hour period.
hour4	Period Filter: End Hours.
intf-name	interface name.
bridge-num	bridge number.
subs-name1	Filter condition: static username, exact match.
subs-name2	Filter Condition: Authentication Username, Exact Match.
addr	Filter conditions: IP, exact match; multiple IPs are separated by ",".
keyword	Filter conditions: filter keywords, support multi-keyword filtering, separate keywords with commas.
rule-name	Filtering condition: Matching rule name, support multiple rule name filtering, different rule names are separated by half-width commas.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query the WEB-BBS audit statistics.

【Configuration Example]】1: Query the WEB-BBS audit statistics of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

```
AC-FS# show web-bbs-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
50
```

【Prompt Information】-

【Platform Description】 ACE series products do not support, other gateway products with built-in storage support; all gateway products without built-in storage are not supported.

16.38 show web-mail-audit detail

Query the detailed information of the WEB-MAIL audit.

show web-mail-audit detail [export] { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name1] [auth-subscriber subs-name2] [ip addr] [direction { in | out | double }] [from keyword1] [to keyword2] [subject keyword3] [rule-name

rule-name] [permit | deny] order-by { time | subscriber | auth-subscriber | internal-ip | direction | send-mail-addr } { asc | desc } [start-item integer1 end-item integer2]

【Parameter Description】

Parameter	Description
hours	recent time period.
yyyy mm dd	year month day.
hh:mm:ss	hours minutes seconds.
hour1	Time period filter: Start hour period.
hour2	Period Filter: End Hours.
hour3	Time period filter: Start hour period.
hour4	Period Filter: End Hours.
intf-name	interface name.
bridge-num	bridge number.
subs-name1	Filter condition: static username, exact match.
subs-name2	Filter Condition: Authentication Username, Exact Match.
addr	Filter conditions: IP, exact match; multiple IPs are separated by ",".
keyword1	Filter by: Email sender keyword.
keyword2	Filter by: Email recipient keywords.
keyword3	Filter condition: Email subject keyword.
rule-name	Filter Condition: Matched Rule Name.
integer1	The starting position in the query result set.
integer2	The end position in the query result set.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query or export the detailed information of WEB-MAIL audit.

【Configuration Example]】1: Query WEB-MAIL audit details from 0:00 on 2016-9-4 to 24:00 on 2016--11-4.

```
AC-FS# show web-mail-audit detail time-range from 2016 9 4 0:0:0 to 2016 11 4 23:59:59 subscriber userA order-by time
desc start-item 1 end-item 20
================================================================================
=========
id: 65

attach_id: 03030336dcc9b73db95d0050 time_stamp: 1477034534
day_time: 2016-10-21 15:22:14
        sip: 3.3.3.54
```

```
usr_grp: /2 group /
usr_name: user 2
plcy_name: _AUDIT_DEFAULT
rule_name: default_audit action:   permit username: userA@21cn.com nickname:
uid:

receiver: userB<userB@163.com>, userC<userC@sina.com> userD<userD@tom.com> subject: Public hospitals medical
phenomenon getting worse + mental hospitals become the worst-hit areas
mail_size: 17059

attach_num:   0 host: mail.21cn.com
url: mail.21cn.com/w2/mail/sendMail.do
......
```

【Prompt Information】-

【 Platform Description 】 ACE series products do not support, other gateway products with built-in storage support; all gateway products without built-in storage are not supported.

16.39 show web-mail-audit stat

Query the statistics of the WEB-MAIL audit.

show web-mail-audit stat { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name1] [auth-subscriber subs-name2] [ip addr] [direction { in | out | double }] [from keyword1] [to keyword2] [subject keyword3] [rule-name rule-name] [permit | deny]

【Parameter Description】

Parameter	Description
hours	recent time period.
yyyy mm dd	year month day.
hh:mm:ss	hours minutes seconds.
hour1	Time period filter: Start hour period.
hour2	Period Filter: End Hours.
hour3	Time period filter: Start hour period.
hour4	Period Filter: End Hours.
intf-name	interface name.
bridge-num	bridge number.
subs-name1	Filter condition: static username, exact match.
subs-name2	Filter Condition: Authentication Username, Exact Match.
addr	Filter conditions: IP, exact match; multiple IPs are separated by ",".
keyword1	Filter by: Email sender keyword.
keyword2	Filter by: Email recipient keywords.
keyword3	Filter condition: Email subject keyword.
rule-name	Filter Condition: Matched Rule Name.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query the statistical information of WEB-MAIL audit.

【Configuration Example]】1: Query the WEB-MAIL audit statistics of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

```
AC-FS# show web-mail-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
50
```

【Prompt Information】-

【Platform Description】 ACE series products do not support, other gateway products with built-in storage support; all gateway products without built-in storage are not supported.

16.40 show web-search-audit detail

Query the detailed information of the WEB-SEARCH audit.

show web-search-audit detail [export] { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name1] [auth-subscriber subs-name2] [ip addr] [keyword keyword] [rule-name rule-name] [permit | deny] order-by { time | subscriber | auth-subscriber | internal-ip | url } { asc | desc } [start-item integer1 end-item integer2]

【Parameter Description】

Parameter	Description
hours	recent time period.
yyyy mm dd	year month day.
hh:mm:ss	hours minutes seconds.
hour1	Time period filter: Start hour period.
hour2	Period Filter: End Hours.
hour3	Time period filter: Start hour period.
hour4	Period Filter: End Hours.
intf-name	interface name.
bridge-num	bridge number.
subs-name1	Filter condition: static username, exact match.
subs-name2	Filter Condition: Authentication Username, Exact Match.
addr	Filter conditions: IP, exact match; multiple IPs are separated by ",".
keyword	Filter conditions: filter keywords, support multi-keyword filtering, separate keywords with commas.
rule-name	Filtering condition: Matching rule name, support multiple rule name filtering, different rule names are separated by half-width commas.
integer1	The starting position in the query result set.
integer2	The end position in the query result set.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query or export the detailed information of WEB-SEARCH audit.

【Configuration Example]】1: Query 0:00 on 2016-9-4 to 24:00 on 2016--11-4, WEB-SEARCH audit details.

```
AC-FS# show web-search-audit detail time-range from 2016 9 4 0:0:0 to 2016 11 4 23:59:59 subscriber userA order-by time
desc start-item 1 end-item 20
==========================================================================

id: 3

time_stamp: 1479883125 day_time: 2016-11-23 14:38:45 sip: 3.3.3.54
dip: 202.108.23.153

sport: 51526 dport: 80
mac_addr: f48e.388f.f50d usr_grp: /
usr_name: 3.3.3.54
plcy_name: _AUDIT_DEFAULT rule_name: default_audit


obj_name: action: permit
app_type:  Baidu Translate
url:
search_word: activitysearch_type: dict.....
```

【Prompt Information】-

【Platform Description】 ACE series products do not support, other gateway products with built-in storage support; all gateway products without built-in storage are not supported.

16.41 show web-search-audit stat

Query WEB-SEARCH audit statistics.

show web-bbs-audit stat { recent hours | time-range from yyyy mm dd hh:mm::ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name1] [auth-subscriber subs-name2] [ip addr] [keyword keyword] [rule-name rule-name] [permit | deny]

【Parameter Description】

Parameter	Description
hours	recent time period.
yyyy mm dd	year month day.
hh:mm:ss	hours minutes seconds.
hour1	Time period filter: Start hour period.

hour2	Period Filter: End Hours.
hour3	Time period filter: Start hour period.
hour4	Period Filter: End Hours.
intf-name	interface name.
bridge-num	bridge number.
subs-name1	Filter condition: static username, exact match.
subs-name2	Filter Condition: Authentication Username, Exact Match.
addr	Filter conditions: IP, exact match; multiple IPs are separated by ",".
keyword	Filter conditions: filter keywords, support multi-keyword filtering, separate keywords with commas.
rule-name	Filtering condition: Matching rule name, support multiple rule name filtering, different rule names are separated by half-width commas.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query the statistical information of WEB-SEARCH audit.

【Configuration Example]】1: Query the WEB-SEARCH audit statistics of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

```
AC-FS# show web-search-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber
userA
50
```

【Prompt Information】-

【Platform Description】 ACE series products do not support, other gateway products with built-in storage support; all gateway products without built-in storage are not supported.

16.42show vid-audit detail

Query the detailed information of virtual identity audit.

show vid-audit detail [export] { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [subscriber subs-name1] [auth-subscriber subs-name2] [type { weibo | weixin }] [uid uid-string] [nickname nick-string] [ip addr1] [mac addr2] order-by { time | subscriber | auth-subscriber |

internal-ip | uid | mac } { asc | desc } [start-item integer1 end-item integer2]

【Parameter Description】

Parameter	Description
hours	recent time period.
yyyy mm dd	year month day.
hh:mm:ss	hours minutes seconds.
hour1	Time period filter: Start hour period.
hour2	Period Filter: End Hours.
hour3	Time period filter: Start hour period.
hour4	Period Filter: End Hours.
subs-name1	Filter condition: static username, exact match.
subs-name2	Filter Condition: Authentication Username, Exact Match.
uid-string	Filter by: Account UID.
nick-string	Filter condition: account nickname.
addr1	Filter conditions: IP, exact match; multiple IPs are separated by ",".
addr2	Filter conditions: MAC address, exact match; multiple addresses are separated by ",".
integer1	The starting position in the query result set.
integer2	The end position in the query result set.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query or export the detailed information of virtual identity audit.

【Configuration Example]】1: Query the virtual identity audit details of user userA from 0:00 on September 4, 2016 to 24:00 on November 4, 2016.

```
AC-FS# show vid-audit detail time-range from 2016 9 4 0:0:0 to 2016 11 4 23:59:59 subscriber userA type msn order-by time
desc start-item 1 end-item 20
================================================================================
========
id: 1
time_stamp: 1479873007 day_time:
2016-11-23 11:50:07 sip: 3.3.3.54
dip: 61.135.185.139
sport: 50311
dport: 80
mac_addr: f48e.388f.f50d usr_grp: /
usr_name: 3.3.3.54
plcy_name: rule_name:
obj_name:
action: permit
username: nickname:
uid: 8cff9d75777a7fbe1413519c
app_type: Baidu post
barvid_action: LOGIN……
```

【Prompt Information】-

【Platform Description】 ACE series products do not support, other gateway products with built-in storage support; all gateway products without built-in storage are not supported.

16.43show vid-audit stat

Query statistics for virtual identity auditing.

show vid-audit stat { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [subscriber subs-name1] [auth-subscriber subs-name2] [type { weibo | weixin }] [uid uid-string] [nickname nick-string] [ip addr1] [mac addr2]

【Parameter Description】

Parameter	Description
hours	recent time period.
yyyy mm dd	year month day.
hh:mm:ss	hours minutes seconds.
hour1	Time period filter: Start hour period.
hour2	Period Filter: End Hours.
hour3	Time period filter: Start hour period.
hour4	Period Filter: End Hours.
subs-name1	Filter condition: static username, exact match.
subs-name2	Filter Condition: Authentication Username, Exact Match.
uid-string	Filter by: Account UID.
nick-string	Filter condition: account nickname.
addr1	Filter conditions: IP, exact match; multiple IPs are separated by ",".
addr2	Filter conditions: MAC address, exact match; multiple addresses are separated by ",".

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query the statistics of virtual identity audit.

【Configuration Example]】1: Query the MSN audit statistics of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

```
AC-FS# show vid-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
type msn
50
```

【Prompt Information】-

【Platform Description】 ACE series products do not support, other gateway products with built-in storage support; all gateway products without built-in storage are not supported.

16.44show https-audit enable

Query the status of the HTTPS audit enable switch.

show https-audit enable

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query the status of the HTTPS audit enable switch.

【Configuration Example]】1: Query the status of the HTTPS audit enable switch.

```
AC-FS#show https-audit enable
{
    "code": 0,
    "msg": "",
    "data": {
        "enable": "on"
    }
}
```

【Prompt Information】-

【Platform Description】 It is supported by all EG series and NBR series products, but not supported by other series of gateway products.

16.45url

Add URL entries to the URL category.

url url-string

Delete the URL entry.

no url url-string

【Parameter Description】

Parameter	Description
url-string	The URL entries contained in the URL category support pattern matching: 1. If the URL contained in the custom website category is a subdirectory under the domain name, all files in the subdirectory will be matched. For example: if the URL is "ietf.org/2006", it will match all the contents in the "ietf.org/2006" directory. 2. If the URL contained in the custom website category is a domain name and does not contain a path, it will match all accesses to the domain name and its subdomains. For example, if the URL is "ietf.org", it will match the "www.ieft.org" ” and access to subdomains such as “download.ietf.org” and “news.ietf.org”.

【Default Configuration】 There is no configuration by default.

【Command Mode】 URL classification configuration mode

【Default Level】 14

【 Usage Guide 】 1: URL pattern matching currently only supports level 2 directories, and users are not allowed to configure "ietf.org/2006/12/1";

2: URL subdomain pattern matching currently only supports level 4 subdomains. If the user configuration is "test.rfc.download.ietf.org", it can only match exact domain names.

【Configuration Example]】 1: Add an entry for the URL classification classA: ietf.org.

```
AC-FS# configure terminal AC-
FS(config)# url-class classA AC-
FS(url-cls-config)# url ietf.org
AC-FS(url-cls-config)#end
```

【Verification】 Use the show running-config command to view the configuration status.

【Prompt Information】 1: If the configured URL format is incorrect, a prompt will be given.

```
AC-FS(config)# url ietf.org/2006/12/1
Format error
```

【Common Mistake】-

【Platform Description】 All gateway series products are supported.

16.46 url-audit

Enable the corresponding URL optimization audit function.

url-audit { exact-filter | except-postfix | except-regexp [regexp] | only-get | optimize-cache [time] }

Turn off the corresponding URL optimization audit function.

no url-audit { exact-filter | except-postfix | except-regexp [regexp] | only-get | optimize-cache [time] }

【Parameter Description】

Parameter	Description
regexp	The Parameter is a regular expression. After this function is enabled, URLs matching the regular expression will not be audited.
time	The Parameter is built in seconds, and when the function is turned on, the same URL is not repeated in time time to And the link page opened from the URL web page.

【Default Configuration】 It is enabled by default, and the command is not displayed. Commands are displayed only after the no command has been executed.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 1: If no regular expression is specified when url-audit except-regexp is enabled, it will be specified as ".*=.*&.*=.*" by default.

2: When url-audit except-postfix is enabled, the following URLs with suffixes, jpg, css, js, gif, png, swf, bmp, ico, ng, dll, GIF, JPG, xml, ini, will not be audited.

3: Enable url-audit optimize-cache, the default time is 30s.

【Configuration Example]】1: Enable only audit HTTP GET.

```
AC-FS# configure terminal
AC-FS(config)# url-audit only-get
AC-FS(config)#end
```

2: Configure URL access that matches the default regular expression (.*=.*&.*=.*) to not be audited.

```
AC-FS# configure terminal
AC-FS(config)# url-audit except-regexp AC-
FS(config)# end
```

3: URL access with suffixes such as configuration pictures is not audited.

```
AC-FS# configure terminal
```

```
AC-FS(config)# url-audit except-postfix
AC-FS(config)# end
```

4: Within the specified 60s, the duplicate URL access of the same IP will not be audited and the links clicked from the URL page will not be audited.

```
AC-FS# configure terminal
AC-FS(config)# url-audit optimize-cache 60 AC-
FS(config)# end
```

【Verification】 Use the show running-config command to view the configuration status.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 All gateway series products are supported.

16.47 url-class

Specify the URL category name and enter the URL category configuration mode.

url-class class-name

Remove URL categorization.

no url-class class-name

【Parameter Description】

Parameter	Description
class-name	The URL taxonomy name.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Use this command to configure URL classification.

【Configuration Example]】1: Add a URL category classA.

```
AC-FS# configure terminal
```

```
AC-FS(config)# url-class classA
AC-FS(url-obj-config)#end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 All gateway series products are supported.

16.48 url-filter-notice

Configure the content displayed on the URL filtering prompt page.

url-filter-notice display [text]

Disable the URL filtering prompt page display function.

no url-filter-notice

【Parameter Description】

Parameter	Description
text	This command allows you to configure what appears on the URL filter prompt page.

【Default Configuration】 Open by default. The default display content is:

"You are forbidden to visit the website, please contact webmaster!"

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Use this command to configure the content displayed on the URL filtering prompt page.

【Configuration Example]】1: Configure the information displayed on the URL filtering prompt page:

```
AC-FS# configure terminal
AC-FS(config)# url-filter-notice displayThe web site you visit has been banned, please contact your administrator! AC-FS(config)#end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 All gateway series products are supported.

16.49 url-object

Specify the URL object name and enter URL object configuration mode.

url-object object-name

Delete the URL object.

no url-object object -name

【Parameter Description】

Parameter	Description
object-name	The URL object name.The maximum length is 40 bytes.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Use this command to configure the URL object. The URL object capacity is 100.

【Configuration Example]】1: Add a URL object objA.

```
AC-FS# configure terminal
AC-FS(config)# url-object objA
AC-FS(url-obj-config)# end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 All gateway series products are supported.

16.50 url-rule

Enable URL default auditing.

url-rule audit-default-enable

Disable URL default auditing.

no url-rule audit-default-enable

Delete all URL rules under the policy group.

url-rule delete-all

Exchange the priority of URL access control rules.

url-rule priority-swap rule-id1 rule-id2

Add URL access control rules to the content audit policy group.

url-rule rule-id url-object url-obj-name time-range time-name action { permit | deny } [audit] [comment

comment-string]

Delete URL access control rules.

no url-rule rule-id

Enable the URL loose whitelist function.

url-rule apply-referer

Disable the URL loose whitelist feature.

no url-rule apply-referer

【Parameter Description】

Parameter	Description
rule-id1	The ID of Rule 1 where the priority is to be exchanged.
rule-id2	The ID of Rule 2 where the priority is to be exchanged.
rule-id	ID identification of the rule, value range (1~200), and a rule capacity of 200.
url-obj-name	The URL object associated with the rule.
time-name	Time object name representing the time period when the rule takes effect.
comment-string	The Description of the rule.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Content audit policy group configuration mode

【Default Level】 14

【Usage Guide】 1: The rule-id of a rule is not allowed to be repeated in the same content audit policy group, but is allowed to be repeated

in different content audit policy groups.

2: The access control rules in a content audit policy group have corresponding priorities, and the rule assigned last has the highest priority.

3: The time-name and url-obj-name associated with the rule may not exist, and the rule will not take effect at this time.

4: The swap priority command is used to swap the priorities of two access control rules. After running this command, you can see that the order of the two rules has changed in show running-config, but the order of the two rules will not appear in show running-config. Order.

5: The default audit can only be configured in the default audit group named _AUDIT_DEFAULT in the policy group, and this command will not take effect if configured in other policy groups.

6: The url-rule apply-referer needs to be matched with the URL audit filtering policy. After the configuration is complete, in addition to matching the corresponding URL, the URL rule will also use the referer Field to match the rule. If you only configure this command without enabling the corresponding URL audit filtering rule, it will have no actual effect. It is mainly used in the URL whitelist policy, which can allow both websites and their sub-sites in the whitelist.

【Configuration Example]】1: Enable URL default auditing.

```
AC-FS# configure terminal
AC-FS(config)# content-policy _AUDIT_DEFAULT AC-FS(cont-
plcy-config)# url-rule audit-default-enable AC-FS(cont-
plcy-config)# end
```

2: Delete all URL rules in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# url-rule delete-all
AC-FS(cont-plcy-config)# end
```

3: Exchange the priority of URL access control rule 10 and rule 20 in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# url-rule priority-swap 10 20
AC-FS(cont-plcy-config)# end
```

4: Add a URL access audit rule to the content audit policy group policyA, which does not allow access to the URL in the URL object url-objA, and needs to audit this type of URL access.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# url-rule 2 url-object url-objA time-range any action deny audit
```

```
AC-FS(cont-plcy-config)# end
```

5: Enable the URL loose whitelist function.

```
AC-FS# configure terminal AC-
FS(config)#url-rule apply-referer AC-
FS(config)#end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】1: If the configured rule-id already exists, a prompt will be given.

```
AC-FS(config)# url-rule 2 url-object url-objA time-range any action deny audit
Rule 2 already exists, please delete it first
```

【Common Mistake】-

【Platform Description】 All gateway series products are supported.

16.51 web-bbs-rule

Enable WEB-BBS default audit function.

web-bbs-rule audit-default-enable

Disable the default audit function of WEB-BBS.

no web-bbs-rule audit-default-enable

Delete all WEB-BBS rules under the policy group.

web-bbs-rule delete-all

Exchange the priority of WEB-BBS access control rules.

web-bbs-rule priority-swap rule-id1 rule-id2

Add WEB-BBS access control rules to the content audit policy group.

web-bbs-rule rule-id time-range time-name [content content-object-name] action { permit | deny } [audit] [comment comment-string]

Delete WEB-BBS access control rules.

no web-bbs-rule rule-id

【Parameter Description】

Parameter	Description
rule-id1	The ID of Rule 1 where the priority is to be exchanged.
rule-id2	The ID of Rule 2 where the priority is to be exchanged.
rule-id	ID identification of the rule, value range (1~200), and a rule capacity of 200.
time-name	Time object name representing the time period when the rule takes effect.
content-object-name	The content object name used by the rule.
comment-string	The Description of the rule.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Content audit policy group configuration mode

【Default Level】 14

【Usage Guide】 1: The rule-id of a rule is not allowed to be repeated in the same content audit policy group, but is allowed to be repeated in different content audit policy groups.

2: The access control rules in a content audit policy group have corresponding priorities, and the rule assigned last has the highest priority.

3: The time-name and content-object-name associated with the rule may not exist, and the rule will not take effect at this time.

4: The swap priority command is used to swap the priorities of two access control rules. After running this command, you can see that the order of the two rules has changed in show running-config, but the order of the two rules will not appear in show running-config. Order.

5: The default audit can only be configured in the default audit group named _AUDIT_DEFAULT in the policy group, and this command will not take effect if configured in other policy groups.

【Configuration Example]】 1: Enable WEB-BBS default auditing.

```
AC-FS# configure terminal
AC-FS(config)# content-policy _AUDIT_DEFAULT
AC-FS(cont-plcy-config)# web-bbs-rule audit-default-enable
AC-FS(cont-plcy-config)# end
```

2: Delete all WEB-BBS rules in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# web-bbs-rule delete-all
AC-FS(cont-plcy-config)# end
```

3: Exchange the priority of WEB-BBS access control rule 10 and rule 20 in policy group policyA.

```
AC-FS# configure terminal
```

```
AC-FS(config)# content-policy policyA
AC-FS(cont-plcy-config)# web-bbs-rule priority-swap 10 20
AC-FS(cont-plcy-config)# end
```

4: Add a WEB-BBS access audit rule to the content audit policy group policyA, filter users to browse WEB-BBS content, and need to audit the browsing information

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# web-bbs-rule 2 time-range any content keyword-group action deny audit
comment DenyInvalidBBS
AC-FS(cont-plcy-config)# end
```

【Verification】 Use the show running-config command to view the configuration status.

【Prompt Information】 1: If the configured rule-id already exists, a prompt will be given.

【Common Mistake】 -

【Platform Description】 ACE series products do not support, other gateway products with built-in storage support; NBR-E series, EG2000F products support, other gateway products without built-in storage are not supported.

16.52 web-mail-rule

Enable WEB-MAIL default audit function.

web-mail-rule audit-default-enable

Disable the default audit function of WEB-MAIL.

no web-mail-rule audit-default-enable

Delete all WEB-MAIL rules under the policy group.

web-mail-rule delete-all

Exchange the priority of WEB-MAIL access control rules.

web-mail-rule priority-swap rule-id1 rule-id2

Add the public part of the WEB-MAIL access control rule to the content audit policy group.

web-mail-rule rule-id time-range time-name [direction { in | out | double }] action { permit | deny } audit [comment comment-string]

Add a further Parameter description of the WEB-MAIL access control rule to the content audit policy group, mainly the keyword matching conditions of the Description rule. This command is optional, if not configured, it means audit all mail information that satisfies the web-mail-rule rule-id time-range command.

web-mail-rule rule-id relation { and | or } [from content-object-name1] [to content-object-name2] [subject content-object-name3] [body content-object-name4] [attachment-name content-object-name5]

Delete the WEB-MAIL access control rule.

no web-mail-rule rule-id

【Parameter Description】

Parameter	Description
rule-id1	The ID of Rule 1 where the priority is to be exchanged.
rule-id2	The ID of Rule 2 where the priority is to be exchanged.
rule-id	ID identification of the rule, value range (1~200), and a rule capacity of 200.
time-name	Time object name representing the time period when the rule takes effect.
comment-string	The Description of the rule.
content-object-name1	Sender keyword, missing item means not match.
content-object-name2	Recipient keyword, missing item does not match the item.
content-object-name3	Message title keyword, missing item indicates that it does not match.
content-object-name4	Message content keyword, missing item means that it does not match.
content-object-name5	Attachment name keyword, missing item does not match.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Content audit policy group configuration mode

【Default Level】 14

【Usage Guide】1: The rule-id of a rule is not allowed to be repeated in the same content audit policy group, but is allowed to be repeated in different content audit policy groups.

2: The access control rules in a content audit policy group have corresponding priorities, and the rule assigned last has the highest priority.

3: The time-name and content-object-name associated with the rule may not exist, and the rule will not take effect at this time.

4: When the rule is configured as blocking, only the or relation in relation will be valid.

5: The swap priority command is used to swap the priorities of two access control rules. After running this command, you can see that the order of the two rules has changed in show running-config, but the order of the two rules will not appear in show running-config. Order.

6: The default audit can only be configured in the default audit group whose policy group name is _AUDIT_DEFAULT, and this command will not take effect if configured in other policy groups.

【Configuration Example]】1: Enable WEB-MAIL default auditing.

```
AC-FS# configure terminal
AC-FS(config)# content-policy _AUDIT_DEFAULT
AC-FS(cont-plcy-config)# web-mail-rule audit-default-enable
AC-FS(cont-plcy-config)# end
```

2: Delete all WEB-MAIL rules in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# web-mail-rule delete-all
AC-FS(cont-plcy-config)# end
```

3: Exchange the priority of WEB-MAIL access control rule 10 and rule 20 in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# web-mail-rule priority-swap 10 20
AC-FS(cont-plcy-config)# end
```

4: Add a WEB-MAIL access control rule to the content audit policy group policyA to allow users to send WEB mail, matching the OBJ-F keyword for the sender, or matching the OBJ-S keyword for the subject.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# web-mail-rule 1 time-range any action permit audit comment mail-audit-1
AC-FS(cont-plcy-config)# web-mail-rule 1 relation or from OBJ-F subject OBJ-S
AC-FS(cont-plcy-config)# end
```

【Verification】 Use the show running-config command to view the configuration status.

【Prompt Information】 1: If the configured rule-id already exists, a prompt will be given.

```
AC-FS(config)# web-mail-rule 1 time-range any action permit audit comment mail-audit-1
Rule 1 already exists, please delete it first
```

2: If the public part of the rule is not configured, and the further Description of the rule is directly configured, a prompt will be given.

```
AC-FS(config)# web-mail-rule 1 relation or from OBJ-F subject OBJ-S
Rule 1 is not exist
```

【Common Mistake】 -

【Platform Description】 ACE series products do not support, other gateway products with built-in storage support; NBR-E series, EG2000F products support, other gateway products without built-in storage are not supported.

16.53 web-search-rule

Enable WEB-SEARCH default audit function.

web-search-rule audit-default-enable

Turn off the default audit function of WEB-SEARCH.

no web-search-rule audit-default-enable

Delete all WEB-SEARCH rules under the policy group.

web-search-rule delete-all

Exchange the priority of WEB-SEARCH access control rules.

web-search-rule priority-swap rule-id1 rule-id2

Add a WEB-SEARCH access control rule to the content audit policy group.

web-search-rule rule-id time-range time-name [content content-object-name] action { permit | deny } [audit] [comment comment-string]

Add a WEB-SEARCH access control rule to the content audit policy group, specifying matching search types.

web-search-rule type { academic | book | dict | html | image | knows | map | music | news | others | shopping | social | stock | video }

Delete the WEB-SEARCH access control rule.

no web-search-rule rule-id

【Parameter Description】

Parameter	Description
rule-id1	The ID of Rule 1 where the priority is to be exchanged.
rule-id2	The ID of Rule 2 where the priority is to be exchanged.
rule-id	ID identification of the rule, value range (1~200), and a rule capacity of 200.
time-name	Time object name representing the time period when the rule takes effect.
content-object-name	The content object name used by the rule.
comment-string	The Description of the rule.
academic	Search for academic.
book	Search for book libraries, and libraries.
dict	Search the dictionary.
html	Search for web pages.
image	Search for pictures.
knows	Search for Know,
map	Search for maps.
music	Search for music.
news	Search for news.
others	Search for other types.
shopping	Search for shopping.
social	Search for social related, such as Weibo, blog.
stock	Search for stock.
video	Search for video.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Content audit policy group configuration mode

【Default Level】 14

【Usage Guide】 1: The rule-id of a rule is not allowed to be repeated in the same content audit policy group, but is allowed to be repeated in different content audit policy groups.

2: The access control rules in a content audit policy group have corresponding priorities, and the rule assigned last has the highest priority.

3: The time-name and content-object-name associated with the rule may not exist, and the rule will not take effect at this time.

4: The swap priority command is used to swap the priorities of two access control rules. After running this command, you can see that the order of the two rules has changed in show running-config, but the order of the two rules will not appear in show running-config. Order.

5: The default audit can only be configured in the default audit group named _AUDIT_DEFAULT in the policy group, and this command will not take effect if configured in other policy groups.

【Configuration Example]】 1: Enable WEB-SEARCH default auditing.

```
AC-FS# configure terminal
AC-FS(config)# content-policy _AUDIT_DEFAULT
AC-FS(cont-plcy-config)# web-search-rule audit-default-enable
AC-FS(cont-plcy-config)# end
```

2: Delete all WEB-SEARCH rules in policy group policyA.

```
AC-FS# configure terminal
```

```
AC-FS(config)# content-policy policyA
AC-FS(cont-plcy-config)# web-search-rule delete-all
AC-FS(cont-plcy-config)# end
```

3: Exchange the priority of WEB-SEARCH access control rule 10 and rule 20 in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# web-search-rule priority-swap 10 20
AC-FS(cont-plcy-config)# end
```

4: Add a WEB-SEARCH access audit rule to the content audit policy group policyA to filter the behavior of users searching for keywords in the keyword-group content object, and the search information needs to be audited

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# web-search-rule 2 time-range any content keyword-group action deny audit
comment DenyInvalidSearch
AC-FS(cont-plcy-config)# end
```

【Verification】 Use the show running-config command to view the configuration status.

【Prompt Information】 1: If the configured rule-id already exists, a prompt will be given.

```
AC-FS(config)# web-search-rule 2 time-range any content keyword-group action deny audit comment
DenyInvalidSearch
Rule 2 already exists, please delete it first
```

【Common Mistake】 -

【Platform Description】 ACE series products do not support, other gateway products with built-in storage support; NBR-E series, EG2000F products support, other gateway products without built-in storage are not supported.

16.54vid-rule

Enable virtual identity default auditing.

vid-rule audit-default-enable

Disable the default auditing function of virtual identities.

no vid-rule audit-default-enable

Delete all virtual identity rules under the policy group.

vid-rule delete-all

Swap the priority of virtual identity audit rules.

vid-rule priority-swap rule-id1 rule-id2

Add a virtual identity audit rule to the content audit policy group.

vid-rule rule-id time-range time-name [content content-object-name] action { permit | deny } [audit] [comment comment-string]

Delete the virtual identity audit rule.

no vid-rule rule-id

【Parameter Description】

Parameter	Description
rule-id1	The ID of Rule 1 where the priority is to be exchanged.
rule-id2	The ID of Rule 2 where the priority is to be exchanged.
rule-id	ID identification of the rule, value range (1~200), and a rule capacity of 200.
time-name	Time object name representing the time period when the rule takes effect.
content-object-name	The content object name used by the rule.
comment-string	The Description of the rule.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Content audit policy group configuration mode

【Default Level】 14

【Usage Guide】1: The rule-id of a rule is not allowed to be repeated in the same content audit policy group, but is allowed to be repeated in different content audit policy groups.

2: The access control rules in a content audit policy group have corresponding priorities, and the rule assigned last has the highest priority.

3: The time-name and content-object-name associated with the rule may not exist, and the rule will not take effect at this time.

4: The swap priority command is used to swap the priorities of two access control rules. After running this command, you can see that the order of the two rules has changed in show running-config, but the order of the two rules will not appear in show running-config. Order.

5: The default audit can only be configured in the default audit group named _AUDIT_DEFAULT in the policy group, and this command will not take effect if configured in other policy groups.

【Configuration Example]】1: Enable virtual identity default auditing.

```
AC-FS# configure terminal
AC-FS(config)# content-policy _AUDIT_DEFAULT
```

```
AC-FS(cont-plcy-config)# vid-rule audit-default-enable
AC-FS(cont-plcy-config)# end
```

2: Delete all virtual identity audit rules in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# vid-rule delete-all
AC-FS(cont-plcy-config)# end
```

3: Exchange the priority of virtual identity audit rule 10 and rule 20 in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# vid-rule priority-swap 10 20
AC-FS(cont-plcy-config)# end
```

4: Add a VID access audit rule to the content audit policy group policyA, filter the logins containing keywords in the keyword group keyword-group, and need to audit this information.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# vid-rule 2 time-range any content keyword-group action deny audit comment
TEST
AC-FS(cont-plcy-config)# end
```

【Verification】 Use the show running-config command to view the configuration status.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 ACE series products do not support, other gateway products with built-in storage support; NBR-E series, EG2000F products support, other gateway products without built-in storage are not supported.

16.55 https-audit enable

Enable HTTPS auditing.

https-audit enable

Disable HTTPS auditing.

no https-audit enable

【Parameter Description】-

【Default Configuration】 It is disabled by default.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】It must be used in conjunction with the rules of each sub-service of content auditing. For example, after enabling the HTTPS audit enable switch, you need to configure URL rules to perform domain name auditing and filtering on HTTPS encrypted websites.

【Configuration Example]】1: Enable the HTTPS audit function.

```
AC-FS# configure terminal
AC-FS(config)# https-audit enable
AC-FS(config)# end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 It is supported by all EG series and NBR series products, but not supported by other series of gateway products.

16.56 url-redirect-rule

Delete all URL redirection rules under the policy group.

url-redirect-rule delete-all

Exchange the priority of URL redirection access control rules.

url-redirect-rule priority-swap rule-id1 rule-id2

Add URL redirection access control rules to the content audit policy group.

url-redirect-rule rule-id time-range time-name from url-1 to url-2 [comment comment-string]

Remove URL redirection access control rules.

no url-redirect-rule rule-id

【Parameter Description】

Parameter	Description
rule-id1	The ID of Rule 1 where the priority is to be exchanged.
rule-id2	The ID of Rule 2 where the priority is to be exchanged.
rule-id	ID identification of the rule, value range (1~200), and a rule capacity of 200.
time-name	Time object name representing the time period when the rule takes effect.
url-1	The url address that requires a redirection.
url-2	Redirected url address.
comment-string	The Description of the rule.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Content audit policy group configuration mode

【Default Level】 14

【Usage Guide】 1: The rule-id of a rule is not allowed to be repeated in the same content audit policy group, but is allowed to be repeated in different content audit policy groups.

2: The URL redirection rules in a content audit policy group have corresponding priorities, and the rule assigned last has the highest priority.

3: The time-name associated with the rule may not exist, and the rule will not take effect at this time.

4: The swap priority command is used to swap the priorities of two URL redirection rules. After running this command, you can see that the order of the two rules has changed in show running-config, but show running-config will not appear. the command.

【Configuration Example]】 1: Delete all URL redirection rules in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# url-redirect-rule delete-all
AC-FS(cont-plcy-config)# end
```

2: Exchange the priority of URL redirection rule 10 and rule 20 in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# url-redirect-rule priority-swap 10 20
AC-FS(cont-plcy-config)# end
```

3: Add a URL redirection rule for the content audit policy group policyA to redirect www.sina.com.cn to www.AC-FS.com.cn.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# url-redirect-rule 2 time-range any from www.sina.com.cn to www.AC-FS.com.cn comment sina-redirect
AC-FS(cont-plcy-config)# end
```

【Verification】 Use the show running-config command to view the configuration status.

【Prompt Information】 1: If the configured rule-id already exists, a prompt will be given.

```
AC-FS(config)# url-redirect-rule 2 time-range any from www.sina.com.cn to www.AC-FS.com.cn comment sina-redirect
Rule 2 already exists, please delete it first
```

【Common Mistake】 -

【Platform Description】 All gateway series products support.

16.57show telnet-audit detail

Query the detailed information of TELNET audit.

show telnet-audit detail [export] { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [subscriber subs-name1] [auth-subscriber subs-name2] [internal-ip addr1] [service-ip addr2] [conn | disconn] [rule-name rule-name] [permit | deny] order-by { time | subscriber | auth-subscriber | internal-ip | service-ip} { asc | desc } [start-item integer1 end-item integer2]

【Parameter Description】

Parameter	Description
hours	recent time period.
yyyy mm dd	year month day.

hh:mm:ss	hours minutes seconds.
subs-name1	Filter condition: static username, exact match.
subs-name2	Filter Condition: Authentication Username, Exact Match.
hour1	Time period filter: Start hour period.
hour2	Period Filter: End Hours.
hour3	Time period filter: Start hour period.
hour4	Period Filter: End Hours.
addr1	Filter conditions: intranet IP, exact match; multiple IPs are separated by ",".
addr2	Filter conditions: server IP , exact match; multiple IPs are separated by ",".
rule-name	Filtering condition: Matching rule name, support multiple rule name filtering, different rule names are separated by half-width commas.
integer1	The starting position in the query result set.
integer2	The end position in the query result set.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query or export the detailed information of TELNET.

【Configuration Example]】1: Query the TELNET audit details of user userA from 0:00 on 2016-9-4 to 24:00 on 2016-11-4.

```
AC-FS# show telnet-audit detail time-range from 2016 11 4 0:0:0 to 2016 11 4 23:59:59 subscriber userA order-by time desc start-item 1 end-item 20
```

```
id: 1
time_stamp: 1480056761
day_time: 2016-11-25 14:52:41
sip: 3.3.3.54
dip: 60.28.228.9
sport: 60141
dport: 23
mac_addr: f48e.388f.f50d
usr_grp: /
usr_name: 3.3.3.54
plcy_name: _AUDIT_DEFAULT
rule_name: default_audit
app_type: telnet
state:connect
.....
```

【Prompt Information】-

【Platform Description】 ACE series products are not supported, other products with built-in storage are supported, and all products without built-in storage are not supported.

16.58 show telnet-audit stat

Query statistics for TELNET auditing.

show telnet-audit stat { recent hours | time-range from yyyy mm dd hh:mm::ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [subscriber subs-name1] [auth-subscriber subs-name2] [internal-ip addr1] [service-ip addr2] [conn | disconn] [rule-name rule-name] [permit | deny]

【Parameter Description】

Parameter	Description
hours	recent time period.
yyyy mm dd	year month day.
hh:mm:ss	hours minutes seconds.
hour1	Time period filter: Start hour period.

hour2	Period Filter: End Hours.
hour3	Time period filter: Start hour period.
hour4	Period Filter: End Hours.
subs-name1	Filter condition: static username, exact match.
subs-name2	Filter Condition: Authentication Username, Exact Match.
addr1	Filter conditions: IP, exact match; multiple IPs are separated by ",".
addr2	Filter conditions: server IP, exact match; multiple IPs are separated by ",".
rule-name	Filtering condition: Matching rule name, support multiple rule name filtering, different rule names are separated by half-width commas.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query the statistics of TELNET audit.

【Configuration Example]】1: Query the TELNET audit statistics of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

```
AC-FS# show telnet-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
50
```

【Prompt Information】-

【Platform Description】 ACE series products are not supported, other products with built-in storage are supported, and all products without built-in storage are not supported.

16.59 show ftp-audit detail

Query the detailed information of ftp audit.

show ftp-audit detail [export] { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [subscriber subs-name1] [auth-subscriber subs-name2] [internal-ip addr1] [file-name keyword] [rule-name rule-name] [permit | deny] order-by { time | subscriber | auth-subscriber | internal-ip } { asc | desc } [start-item integer1 end-item integer2]

【Parameter Description】

Parameter	Description
hours	recent time period.

yyyy mm dd	year month day.
hh:mm:ss	hours minutes seconds.
subs-name1	Filter condition: static username, exact match.
subs-name2	Filter Condition: Authentication Username, Exact Match.
hour1	Time period filter: Start hour period.
hour2	Period Filter: End Hours.
hour3	Time period filter: Start hour period.
hour4	Period Filter: End Hours.
keyword	Filter conditions: match file name keywords, support multi-keyword filtering, and separate keywords with commas
rule-name	Filtering condition: Matching rule name, support multiple rule name filtering, different rule names are separated by half-width commas
addr1	Filter conditions: intranet IP, exact match; multiple IPs are separated by ",".
integer1	The starting position in the query result set.
integer2	The end position in the query result set.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query or export the detailed information of FTP audit.

【Configuration Example]】1: Query the FTP audit details of user userA from 0:00 on 2016-9-4 to 24:00 on 2016-11-4.

```
AC-FS# show ftp-audit detail time-range from 2016 11 4 0:0:0 to 2016 11 4 23:59:59 subscriber userA
order-by time desc start-item 1 end-item 20
```

```
id: 1
time_stamp: 1480056761
day_time: 2016-11-25 14:52:41
```

```
sip: 3.3.3.54
dip: 60.28.228.9
sport: 60141
dport: 21
mac_addr: f48e.388f.f50d
file  name:aaa.txt
usr_grp: /
usr_name: 3.3.3.54
plcy_name: _AUDIT_DEFAULT
rule_name: default_audit
state:upload
action:permit
```

【Prompt Information】-

【Platform Description】 ACE series products are not supported, other products with built-in storage are supported, and all products without built-in storage are not supported.

16.60 show ftp-audit stat

Query statistics for ftp auditing.

show ftp-audit stat { recent hours | time-range from yyyy mm dd hh:mm::ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [subscriber subs-name1] [auth-subscriber subs-name2] [internal-ip addr1] [file-name keyword] [rule-name rule-name] [permit | deny]

【Parameter Description】

Parameter	Description
hours	recent time period.
yyyy mm dd	year month day.
hh:mm:ss	hours minutes seconds.
hour1	Time period filter: Start hour period.
hour2	Period Filter: End Hours.
hour3	Time period filter: Start hour period.
hour4	Period Filter: End Hours.
subs-name1	Filter condition: static username, exact match.

subs-name2	Filter Condition: Authentication Username, Exact Match.
addr1	Filter conditions: intranet IP, exact match; multiple IPs are separated by ",".
keyword	Filter conditions: match file name keywords, support multi-keyword filtering, and separate keywords with commas.
rule-name	Filtering condition: Matching rule name, support multiple rule name filtering, different rule names are separated by half-width commas.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query the FTP audit statistics.

【Configuration Example]】1: Query the FTP audit statistics of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

```
AC-FS# show ftp-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
50
```

【Prompt Information】-

【Platform Description】 ACE series products are not supported, other products with built-in storage are supported, and all products without built-in storage are not supported.

16.61 file-rule

Delete all FILE rules under the policy group.

file-rule delete-all

Swap the priority of FILE access control rules.

file-rule priority-swap rule-id1 rule-id2

Add a FILE access control rule to the content audit policy group.

file-rule rule-id time-range time-name action { permit | deny } [audit] [comment comment-string]

file-rule rule-id relation { and | or } [file-name content-obj-string1] [file-type content-obj-string2]

Remove the FILE access control rule.

no file-rule rule-id

【Parameter Description】

Parameter	Description
rule-id1	The ID of Rule 1 where the priority is to be exchanged.
rule-id2	The ID of Rule 2 where the priority is to be exchanged.
rule-id	ID identification of the rule, value range (1~200), and a rule capacity of 200.
time-name	Time object name representing the time period when the rule takes effect.
comment-string	The Description of the rule.
content-obj-string1	File name keyword.
content-obj-string2	File type keyword.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Content audit policy group configuration mode

【Default Level】 14

【Usage Guide】 1: The rule-id of a rule is not allowed to be repeated in the same content audit policy group, but is allowed to be repeated in different content audit policy groups.

2: The access control rules in a content audit policy group have corresponding priorities, and the rule assigned last has the highest priority.

3: The time-name associated with the rule may not exist, and the rule will not take effect at this time.

4: The swap priority command is used to swap the priorities of two access control rules. After running this command, you can see that the order of the two rules has changed in show running-config, but the order of the two rules will not appear in show running-config. Order.

【Configuration Example】 1: Delete all FILE rules in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# file-rule delete-all
AC-FS(cont-plcy-config)# end
```

2: Exchange the priority of FILE access control rule 10 and rule 20 in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# file-rule priority-swap 10 20
AC-FS(cont-plcy-config)# end
```

3: Add a FILE access audit rule to the content audit policy group policyA to filter the filename behavior, and the information needs to be audited.

```
AC-FS# configure terminal
AC-FS(config)# content-policy policyA
AC-FS(cont-plcy-config)# file-rule 2 time-range any action deny audit comment TEST
AC-FS(cont-plcy-config)# file-rule 2 relation or file-name 1: Tip is given if the configured rule-id already exists.AC-FS(cont-plcy-config)# end
```

【Verification】 Use the show running-config command to view the configuration status.

【Prompt Information】 1: If the configured rule-id already exists, a prompt will be given.

【Common Mistake】 -

【Platform Description】 ACE series products do not support, other gateway products with built-in storage support; other gateway products without built-in storage are not supported.

16.62 content-audit attach-to-elog enable

Enable attachment upload elog function.

content-audit attach-to-elog enable

Disable the attachment upload elog function.

no content-audit attach-to-elog enable

【Parameter Description】 -

【Default Configuration】 It is disabled by default.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Valid in NPE mode.

【Configuration Example]】1: In NPE mode, enable the elog function of uploading attachments.

```
AC-FS# configure terminal
AC-FS(config)# content-audit attach-to-elog enable AC-FS(config)#
end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 EG2000XE/UE, EG3000XE/UE support, other gateway products do not support.

17 IPSEC-IKE

17.1authentication (IKE policy)

Specifies the authentication method for the IKE policy.

authentication { pre-share }

Restore Default Configuration.

no authentication

【Parameter Description】

Parameter	Description
pre-share	Pre-shared key validation.

【Default Configuration】 The default is pre-shared key authentication.

【Command Mode】 IKE policy configuration mode.

【Default Level】 14

【Usage Guide】At present, the authentication method in the IKE negotiation policy adopts the pre-shared key certificate by default.

【Configuration Example]】1: Configure an IKE policy with a priority of 10 and use the pre-shared key for authentication.

```
AC-FS(config)# crypto isakmp policy 10
AC-FS(isakmp-policy)#authentication pre-share
```

【Verification】-

【Prompt Information】-

【Platform Description】 -

17.2 clear crypto isakmp

Clear running IKE SAs.

clear crypto isakmp [connection-id]

【Parameter Description】

Parameter	Description
connection-id	ID number of the IKE SA. The default is to clear all existing IKE SAs. The value range is <0-65535>.

【Command Mode】 Privileged mode.

【Default Level】 14

【Usage Guide】 Generally, only a specific IKE SA is cleared. You can first use the show crypto isakmp sa command to check the ID number of the SA you want to clear, and then use clear crypto isakmp to clear a specific SA with ID. IKE Security Association. .

【Configuration Example】1: Clear all IKE SAs.

```
AC-FS# clear crypto isakmp
```

【Prompt Information】-

【Platform Description】 -

17.3 clear crypto log

Clear the login and logout logs of IPSec VPN.

clear crypto log

【Parameter Description】 -

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】Clear IPSec VPN login and logout logs.

```
AC-FS # clear crypto log
```

【Prompt Information】-

【Common Mistake】 This indicates that the ipsec process is writing or reading the log file and the log file cannot be deleted at this time

```
AC-FS # clear crypto log

ipsec is writing or reading log now, can not delete file
```

【Platform Description】 -

17.4 clear crypto sa

Clear IPSec SA.

clear crypto sa

Clear the IPSec SA of the corresponding remote peer based on IP or host name.

clear crypto sa peer { ip-address | peer-name }

Clear the IPSec SA corresponding to the remote peer according to the encryption map name.

clear crypto sa map map-name

Clear the IPSec SA corresponding to the remote peer according to the IP address and security parameter index.

clear crypto sa spi destination-address { ah | esp } spi

【Parameter Description】

Parameter	Description
ip-address	The IP address of the distal counterpart.
peer-name	Host name of the distant peer.
map-name	Encrypt the mapping name.
destination-address	The IP address of the local or remote counterpart.
spi	Specify a secure Parameter index with a value range of <0-4294967295>.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 1. The above commands are used to clear IPSec SAs. If keywords such as peer, map, spi are not used, all IPSec SAs will be

deleted by default.

2. If SAs are established through IKE, they will be cleared. When the interface detects that there is a packet that activates IPSec, IPSec renegotiates a new SA. If the SA was created manually, the SA will be cleared and re-established immediately.

3. The new Parameter is configured, which only works on the subsequently negotiated SA, and will not affect the existing SA. In order for the new Parameter to act on the existing SA, this command can be used to clear the existing SA and perform renegotiation.

4. If the SA is cleared, the communication will be interrupted. In order not to interrupt the communication of other IPSec alliances, you should use peer, map, and spi to specify a specific SA.

5. Of course, if there is only one SA, or other SAs have no data to communicate, all SAs can be cleared for renegotiation.

【Configuration Example]】 1: Clear all SAs.

```
AC-FS# clear crypto sa
```

【Prompt Information】 -

【Platform Description】 -

17.5 Crypto dynamic-map

Create a dynamic crypto map entry and enter crypto map configuration mode.

crypto dynamic-map dynamic-map-name dynamic-seq-num

Delete a crypto map set or entry.

no crypto dynamic-map dynamic-map-name [dynamic-seq-num]

【Parameter Description】

Parameter	Description
dynamic-map-name	Specifies the name of the cryptographic mapping set.
dynamic-seq-num	Specifies the entry number for the encryption map.Range ranges from 1 to 65,535

【Default Configuration】 No dynamic encryption map exists.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】

【Configuration Example】-

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.6 Crypto IPSec df-bit

Set the DF value of the encapsulation header for all interfaces.

crypto IPSec df-bit { clear | set | copy }

【Parameter Description】

Parameter	Description
clear	The external IP header will clear the DF Bit, and the device may slice messages and add IPSEC packages.
set	The outer IP header will set the DF bit to 1, however if the DF bit of the original IP header is cleared, the device may fragment the packet.
copy	The device takes the original DF Bit value as the DF Bit value of the external header and the copy is the default.

【Default Configuration】 The command is disabled by default.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】With the clear setting in tunnel mode IPSEC, you can send packets larger than the MTU value, or you don't know how big the MTU is.

If this command is not enabled with an explicit setting, the device will use copy as the default.

【Configuration Example】1: Clear DF Bit on all interfaces.

```
AC-FS(config)# crypto IPSec df-bit clear
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.7crypto IPSec multicast disable

Disable IPSec processing for multicast and broadcast packets.

crypto IPSec multicast disable

Enable IPSec processing for multicast and broadcast packets.

no crypto IPSec multicast disable

【Parameter Description】-

【Default Configuration】 If it is not configured, and the ACL contains multicast and broadcast packets, it will be processed by IPSec.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 If you do not need to perform IPSec processing on multicast and multicast packets, configure this command to skip IPSec processing.

【Configuration Example]】1: Complete the configuration to disable IPSec processing of multicast and broadcast packets.

```
AC-FS(config)# crypto IPSec multicast disable
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.8 Crypto IPSec optional

Turn off IPSec security checks.

crypto IPSec optional

Turn on IPSec Security Check.

no crypto IPSec optional

【Parameter Description】-

【Default Configuration】 By default, this command is disabled.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 The security check itself has a large resource overhead. Disabling this function can save CPU resources. In the l2tp over IPSec model, l2tp can specify the mandatory IPSec function, and can also realize that packets must be encrypted by IPSec before passing. It can be used in combination according to actual needs.

【Configuration Example]】1: Cancel the security check.

```
AC-FS(config)# crypto IPSec optional
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.9crypto IPSec profile (global IPSec-profile)

Create or modify a Profile's crypto map.

crypto IPSec profile profile-name

Cancel a Profile's cryptographic map or entry.

no crypto IPSec profile profile-name

【Parameter Description】

Parameter	Description
profile-name	The name of the Profile Encryption Map collection.

【Default Configuration】 There is no encryption map.

【Command Mode】 Global mode, use this command to enter Profile encryption map configuration mode.

【Default Level】 14

【Usage Guide】When encrypting and protecting data on a tunnel interface, the encryption map of the profile needs to be defined first, and then applied to the tunnel interface. The encrypted communication parameters need to be defined in the Profile encryption mapping table, mainly including the following parameters:

1. Which IPSec security policies should be applied to these communications: Select from a list of one or more transform sets.

2. The life cycle of the security alliance.

3. Whether the SA is established manually or through IKE.

4. If it is an IPV6, IPSEC-IPV4, and IPSEC-IPV6 tunnel, you need to formulate an ACL that negotiates permit any.

Apply the tunnel's encryption map set to the tunnel interface, so that all IP traffic through this interface will be encrypted by the encryption map set applied on the interface. After the configuration is complete, the IKE negotiation is automatically initiated, or the IKE negotiation is triggered when a packet is received from the interface. The policy of Description in the encryption map entry will be used in the negotiation process of the SA. In order to enable the smooth progress of IPSec between two IPSec peers, the tunnel encryption map entries of the two peers must contain compatible configuration statement. When two peers try to establish a security association, both parties must have at least one encryption map entry compatible with one encryption map entry of the other peer and at least meet the following conditions:

1. The crypto map entry must contain a compatible cryptographic access list (such as a mirror image access list).

2. Encryption map entries on both sides must determine the peer address of the other party (unless the peer is using a dynamic encryption map).

3. Encryption map entries must have at least one identical transformation.

4. Only one set of cryptographic maps is applied to a single interface. The encryption map set contains IPSec/IKE. If one of the following situations exists, multiple encryption map entries must be created for an interface: 1. If different data flows on this interface will be sent by

different IPSec peers to be processed.

Multiple crypto map entries must be created for an interface if one of the following conditions exists:

1. If different data flows on this interface will be handled by different IPSec peers.

2. If you want to apply different IPSec security to different types of communication (to the same or different peers); Communications are both authenticated and encrypted. In this case, the different types of communication should be defined in two different access lists, and a separate crypto map entry must be created for each crypto access list.

【Configuration Example]】1: The minimum configuration of the Profile encryption map collection, the profile name is testprofile, and the transformation collection name is mytest.

```
AC-FS(config)# crypto IPSec profile testprofile
AC-FS(config-crypto-map)# set transform-set myset
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.10crypto IPSec security-association lifetime

Modify the global lifetime value used in IPSec SA negotiation.

crypto IPSec security-association lifetime { seconds seconds | kilobytes kilobytes }

Restore the lifetime to default values.

no crypto IPSec security-association lifetime { seconds | kilobytes }

【Parameter Description】

Parameter	Description
seconds seconds	SA timeout (seconds). The default is 3600 seconds (1 hour). It can be configured to 0, which means that the time-out function is not enabled. Range 0, or 120 seconds to 86400 seconds.
kilobytes kilobytes	Security Association timeout traffic (in kilobytes). The default is 4,608,000KB. It can be configured to 0, which means that the byte timeout function is not enabled. Range 0,

	or 2560KB to 536870912KB.

【Default Configuration】 3600 seconds (1 hour) and 4,608,000KB (1 hour of communication at a rate of 10MB per second).

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 1. Sec Security Alliance encrypted communication is based on the use of a shared key. To ensure security, the SA will time out after a certain amount of time or traffic, renegotiate, and use a new shared key. When a device is negotiating an SA, the smaller one of the lifetime values proposed by the peer and configured on the local device is used as the lifetime of the new SA.

2. There are two types of cycles: time life cycle and traffic life cycle. Whichever of the two life cycles expires first, the SA will time out. If the global lifetime is changed, the change only affects the new SA that is subsequently negotiated, and will not affect the existing SA. If you want the new settings to take effect as soon as possible, you can use the clear crypto sa command to clear some or all of the contents of the SA database.

3. To change the global time lifetime, use the command crypto IPSec security-association lifetime seconds. The time lifetime specifies that the security association times out after a certain number of seconds. To modify the global traffic lifetime, use the command crypto IPSec security-association lifetime kilobytes. The traffic lifetime specifies the timeout after a certain amount of traffic (in KB) encrypted by the SA using the SA key.

4. The shorter the period value, the more difficult it is for an attack to crack the key to succeed, because less data encrypted with the same key is used by the attacker for analysis. However, the shorter the lifetime, the more CPU processing time is used to establish a new security association. A security association established by hand has no life cycle.

5. The working principle of the cycle: After a certain time (specified by the seconds keyword) or a certain byte of data traffic (specified by the kilobytes keyword) has passed, whichever of these two things happens first, the SA (and the corresponding key) will time out. The new SA starts to negotiate before the lifetime limit of the original SA is reached, so as to ensure that a new SA can be used when the original SA expires. The new SA starts negotiating 30 seconds before the seconds lifetime expires, or when the data traffic through this tunnel is 256KB away from the kilobytes lifetime (whichever comes first). If there is no communication through this tunnel in the whole life cycle of an SA, the negotiation of a new SA will not be performed when the SA times out. Correspondingly, a new SA will only begin negotiating when IPSec sees a packet that should be protected.

6. The time life cycle and the traffic life cycle cannot be zero at the same time, otherwise the negotiation cannot be successful. The local configuration is not checked and needs to be guaranteed by the user.

【Configuration Example]】1: Set the time period of IPSec SA to 2500 seconds, and set the traffic life cycle to 2304000KB (communication at 10MB rate for half an hour).

```
AC-FS(config)# crypto IPSec security-association lifetime seconds 2500
AC-FS(config)# crypto IPSec security-association lifetime kilobytes 2304000
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

17.11crypto IPSec security-association lifetime not_based_on initiator

Modify the negotiation and matching rules of the IPsec second-stage life cycle, that is, the final negotiation result of the second-stage life cycle is the smaller of the branch life cycle and the headquarters life cycle.

crypto IPSec security-association lifetime not_based_on initiator

Restore the default matching method of the second-stage life cycle: the final negotiation result is subject to the branch.

no crypto IPSec security-association lifetime { seconds | kilobytes }

【Parameter Description】-

【Default Configuration】 In the second stage of the life cycle, the life cycle of the default branch is used as the final negotiation result.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】By default, the negotiation result of the second-stage life cycle is based on the branch, that is, both the headquarters and the branch use the value configured by the branch as the second-stage life cycle. This instruction can be used to modify the matching rules of the second-stage life cycle, that is, to use the smaller of the values configured by the branch and the headquarters as the final negotiation result.

【Configuration Example]】1: Modify the matching rules of the second-stage life cycle.

```
AC-FS(config)# crypto IPSec security-association lifetime not_based_on initiator
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.12crypto IPSec security-association replay disable

Anti-replay switch command, set to not check retransmission message mode.

crypto IPSec security-association replay disable

Set to check retransmission message mode.

no crypto IPSec security-association replay disable

【Parameter Description】-

【Default Configuration】 The default replay check is enabled by default, and is not displayed by default.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】After the command is enabled, it does not check the packet retransmission, which can improve the packet processing efficiency, and at the same time, the possibility of being attacked by DOS is increased.

【Configuration Example]】1: Disable retransmission packet checking.

```
AC-FS(config)# crypto IPSec security-association replay disable
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.13 crypto IPSec transform-set

Defines the set of transformations used by the security association.

crypto IPSec transform-set transform-set-name transform1 [transform2 [transform3]]

Deletes a transform collection.

no crypto IPSec transform-set transform-set-name

【Parameter Description】

Parameter	Description
transform-set-name	The name of the transformation set.
transform1, transform2	For the security protocols and algorithms used by the security alliances, please refer to the security configuration guidance.
transform3	-

【Default Configuration】 No transformation set.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 1. A collection is a combination of security protocols, algorithms, and other settings that will be used for IPSec-protected communications. During IPSec SA negotiation, peers must use the same specific set of transforms to protect specific data flows.

2. Configure multiple transform sets, and then specify one or more of these transform sets in the crypto map entry. The set of transformations defined in the crypto map entry are used to negotiate IPSec security associations to protect those data flows specified by the access list corresponding to the crypto map entry. During the negotiation process, both peers look for an identical set of transformations that are available on both peers. When such a set of transformations is found, this set will be selected and applied to protected communications as part of the IPSec security association of both peers.

3. The SA is established manually. Since the manually established SA does not negotiate Parameter, the peers at both ends must specify the same transformation set.

【Configuration Example]】1: Define the transformation set, and the protection method is ESP-DES-MD5 (encryption and authentication services are provided).

```
AC-FS(config)# crypto IPSec transform-set myset esp-des esp-md5-hmac
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.14 crypto isakmp enable

To use IKE for IPSec SA negotiation, IKE must be enabled first.

crypto isakmp enable

IKE is prohibited.

no crypto isakmp enable

【Parameter Description】-

【Default Configuration】 IKE is enabled by default.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】By default, IKE is enabled, so if you want to use IKE for IPSec SA negotiation, it is not necessary to use this command. If you do not use IKE for IPSec SA negotiation, you can use the no form of this command to disable IKE.

【Configuration Example】1: Enable IKE.

```
AC-FS(config)# crypto isakmp enable
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.15 crypto isakmp keepalive

Send peer detection messages to remote peers.

crypto isakmp keepalive secs [on-demand | periodic]

crypto isakmp keepalive secs retries [on-demand | periodic]

Disable the peer detection message function.

no crypto isakmp keepalive

【Parameter Description】

Parameter	Description
secs	Tunnel survival time, which range from 5 to 3600s.
retries	Time interval from 2 to 60 seconds.
on-demand	Send messages in the free time of the forwarding message.
periodic	Send messages by the configuration interval.

【Default Configuration】 The peer detection message is not sent.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Use crypto isakmp keepalive to make the device periodically send dead peer detection messages to the remote peer to find out whether the remote peer still exists.

【Configuration Example]】 1: Configure the tunnel idle time to 60 seconds, the retransmission interval to 5 seconds, and the on-demand mode.

```
AC-FS(config)# crypto isakmp keepalive 60 5 on-demand
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

17.16 crypto isakmp key

Specifies the pre-shared key used for IKE negotiation.

crypto isakmp key { 0 | 7 } keystring { hostname peer-hostname | address peer-address [mask] }

Deletes the specified pre-shared key.

no crypto isakmp key { 0 | 7} keystring { hostname peer-hostname | address peer-address [mask] }

【Parameter Description】

Parameter	Description
0	7	0 Display plaintext for the key 7 display plaintext for the key.
keystring	Pre-shared key string, with up to 128 characters.
peer-hostname	Host name of the remote peer.
peer-address	The IP address of the remote peer body.
mask	The address mask when the specified IP address is the address of a network segment.

【Default Configuration】 No pre-shared password is specified.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 IKE generally uses pre-shared negotiation. In order for IKE to successfully establish an IKE SA, this command must be used to configure the same pre-shared key on the two communicating peers. If the specified peer is a network segment, use mask to identify its subnet mask. When both peer-address and Mask are 0.0.0.0, the default pre-shared key is configured.

【Configuration Example]】1: Specify the pre-shared key for IKE negotiation with peer 172.16.1.1 as mysecret.

```
AC-FS(config)# crypto isakmp key 0 mysecret address 172.16.1.1
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.17 crypto isakmp limit disable

Disable IKE negotiation rate limit function.

crypto isakmp limit disable

Enable IKE negotiation rate limit function.

no crypto isakmp limit disable

【Parameter Description】-

【Default Configuration】 By default, the negotiation rate limit function of IKE is enabled, and the negotiation rate is 1000.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Disable IKE negotiation rate limit function.

【Configuration Example】1: Disable the IKE negotiation rate limit function.

```
AC-FS(config)# crypto isakmp limit disable
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.18 Crypto isakmp limit rate

Limit the negotiation rate of IKE, that is, set the maximum number of tunnels negotiating at the same time.

crypto isakmp limit rate numbers

Cancel the set speed limit rate and restore the default value.

no crypto isakmp limit rate

【Parameter Description】

Parameter	Description
numbers	Set speed limit rate.

【Default Configuration】 By default, the rate limit is 1000, which means that 1000 ipsec tunnels can be negotiated at the same time.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】When thousands of tunnels are negotiated at the same time, the negotiation may fail to converge or the convergence may be slow, and the entire negotiation process may take several hours or even longer. Based on this deficiency, this command is used to limit the negotiation rate, to ensure that the number of tunnels being negotiated is controlled within a certain range, and to improve the negotiation efficiency.

【Configuration Example】1: Configure the negotiation rate of IKE.

```
AC-FS(config)# crypto isakmp limit rate 500
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.19 crypto isakmp mode-detect

When the local security gateway fails to complete the IKE negotiation initiated by the peer in the main mode, it automatically negotiates in the active mode.

crypto isakmp mode-detect

Turn off auto-aggressive mode.

no crypto isakmp mode-detect

【Parameter Description】-

【Default Configuration】 If there is no configuration, only the main mode is used for negotiation.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】Currently, there are many manufacturers of security products. The implementation of each manufacturer is not uniform. However, there are only two working modes in the first stage of IKE negotiation. When the other party initiates IKE negotiation, the negotiation is automatically completed in the aggressive mode.

【Configuration Example]】1: Automatically identify the negotiation initiated in aggressive mode.

```
AC-FS(config)# crypto isakmp mode-detect
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.20crypto isakmp nat keepalive

Configure nat keepalive sending interval.

crypto isakmp nat keepalive secs

Cancel the configured nat keepalive sending interval and restore the default sending interval.

no crypto isakmp nat keepalive

【Parameter Description】

Parameter	Description
secs	Tunnel survival time, which range from 5 to 3600s.

【Default Configuration】5 minutes.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】Support RFC3947, IPSEC NAT-t, use the method of adding UDP header to solve the problem of NAT penetration. In order to avoid the nat connection timeout, it is necessary to use the keepalive method to send the message. Configure the crypto isakmp nat keepalive command to specify the keepalive sending interval configured by the user. If it is not configured, the default time is 5 minutes.

【Configuration Example]】1: Configure the tunnel keepalive to send packets every 1 minute.

```
AC-FS(config)# crypto isakmp nat keepalive 60
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.21 crypto isakmp nat-traversal disable

Turn off the nat-traversal feature.

crypto isakmp nat-traversal disable

Enable nat-traversal function.

no crypto isakmp nat-traversal disable

【Parameter Description】-

【Default Configuration】 By default, nat-traversal is enabled.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】Some manufacturers implement the protocol, and there is a compatibility problem with the nat-traversal function support. In special cases, the nat-traversal function can be turned off to achieve interoperability.

【Configuration Example]】1: Disable the nat-traversal function.

```
AC-FS(config)# crypto isakmp nat-traversal disable
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.22crypto isakmp next-payload disable

Disable the next-payload check option.

crypto isakmp next-payload disable

Turn on the next-payload check option.

no crypto isakmp next-payload disable

【Parameter Description】-

【Default Configuration】 By default, if there is an unrecognized doi information, it will be considered that the negotiation cannot continue, and a failure will be returned.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】After the next-payload check is turned off, the unrecognized doi Field is ignored, and the negotiation continues. However,

if the reserved Field is not 0, or the length of the Field does not match, a failure will still be returned.

【Configuration Example]】 1: Disable next-payload checking.

```
AC-FS(config)# crypto isakmp next-payload disable
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

17.23 crypto isakmp peer

In the case of multiple peers, specify the first peer to initiate negotiation.

crypto isakmp peer { bind | random }

Cancel the specified priority of the first peer that initiates negotiation.

no crypto isakmp peer

【Parameter Description】

Parameter	Description
bind	Only valid in the 3G environment. The 3G card is configured with multi-peer dial-up and is bound to the IPSec dial-up peer address. According to the configuration sequence, the first group of dial-up configurations corresponds to the first peer configuration.
random	The peer of the first attempt at negotiation was randomly selected.

【Default Configuration】 By default, according to the configuration order, try from the first peer.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 When used together with 3G link, 3G dial-up is configured with multiple groups of dial-up addresses, which correspond

one-to-one with the peer configuration in the IPSec map, and the peer binding function can be turned on to speed up the dial-up speed. Otherwise, you need to retry many times to find the current corresponding peer, and the time to establish the tunnel for the first time will be relatively long.

【Configuration Example】 1: Enable random selection of tunnel connection address.

```
AC-FS(config)# crypto isakmp peer random
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

17.24 crypto isakmp policy

Define an IKE policy with a certain priority and enter the IKE policy configuration mode.

crypto isakmp policy priority

Delete a priority policy.

no crypto isakmp policy priority

【Parameter Description】

Parameter	Description
priority	The priority of the IKE policy. Use an integer from 1 to 10000, with 1 being the highest priority and 10000 the lowest.

【Default Configuration】 There is no default priority.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Use this command to specify the parameters of IKE SA during IKE negotiation. Execute this command to enter the IKE policy configuration mode. In IKE policy configuration mode, the following parameters can be set:

encryption(IKE policy) : default=56 bits DES-CBC

hash(IKE policy) : default=SHA-1

authentication(IKE policy) : default=RSA signature

group(IKE policy) : default=768 bits

Diffie-Hellmanl lifetime(IKE policy) : default=86400 seconds (1 day)

If a Parameter value is not specified, the default value of that Parameter will be used. Multiple IKE policies can be configured on the device. At the beginning of IKE negotiation, it will try to find the common policy configured on both ends, starting with the highest priority policy specified on the remote peer.

【Configuration Example]】1: Configure an IKE policy with a priority of 100.

```
AC-FS(config)# crypto isakmp policy 100 AC-
FS(isakmp-policy)# authentication pre-share AC-
FS(isakmp-policy)# encryption des AC-FS(isakmp-
policy)# group  2
AC-FS(isakmp-policy)# hash  sha
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.25 crypto isakmp vendorid disable

Disable FS vendor information during IKE negotiation.

crypto isakmp vendorid disable

Open the FS manufacturer information during the IKE negotiation process.

crypto isakmp vendorid disable

【Parameter Description】-

【Default Configuration】 By default, FS manufacturer information is included in the IKE negotiation process.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】During the IKE negotiation process, some manufacturers fail to recognize the private VID, resulting in failure of the negotiation. You can use this command to disable the sending of the VID information of FS manufacturers.

【Configuration Example]】1: Disable vendorid during negotiation.

```
AC-FS(config)# crypto isakmp vendorid disable
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.26 Crypto map (global IPSec)

Create or modify a crypto map.

crypto map map-name seq-num { ipsec-manual | ipsec-isakmp [dynamic dynamic-map-name] }

Cancel a crypto map or entry.

no crypto map map-name [seq-num]

【Parameter Description】

Parameter	Description
map-name	The name of the encrypted map collection.
seq-num	The serial number of the encrypted mapping entries.Values range from 1 to 65,535.
IPSec-manual	Specifies the mapping entries to establish a manual IPSec security alliance.
IPSec-isakmp	Specifies the mapping entry to establish the IPSec security alliance for the IKE negotiation.
dynamic-map-name	Specifies the name of the dynamic encryption map set that serves as a policy template.

【Default Configuration】 There is no encryption map.

【Command Mode】 Global mode, use this command to enter encryption map configuration mode.

【Default Level】 14

【Usage Guide】To use IPSec to encrypt and protect data, you must first define an encryption map, and then apply the encryption map to a specific interface. Define the parameters of encrypted communication in the encryption map, mainly including the following parameters:

1. Communication should be protected by IPSec: Associate the configured encrypted access list.

2. Where will the IPSec-protected traffic be sent: who is the remote IPSec peer.

3. The local address used for IPSec communication: apply the encryption map set to the interface, and IPSec uses the address of the communication interface as the address of the local peer.

4. Which IPSec security policies should be applied to these communications: Select from a list of one or more transform sets.

5. The life cycle of the security alliance.

6. Whether the SA is established manually or through IKE.

Crypto-map entries with the same crypto-map name (but different map sequence numbers) form a crypto-map set. Apply the crypto map set to the interface, so that all IP traffic through this interface will be judged by the crypto map set applied on the interface. If an encryption map entry finds outbound IP communication that should be protected, and the encryption map specifies the use of IKE, it will negotiate with the remote peer according to the parameters contained in the encryption map entry; if the encryption map entry If a manually created SA is specified, an SA must have been established during configuration. Regardless of manual establishment or IKE negotiation, as long as the SA is successfully established, the data will be encrypted and transmitted. If the SA negotiation fails, the data will be discarded.

The policy described in the encryption map entry will be used in the negotiation process of the SA. In order for the IPSec between two IPSec peers to proceed smoothly, the encryption map entries of the two peers must contain mutually compatible configurations statement. When two peers try to establish a security association, both parties must have at least one encryption map entry compatible with one encryption map entry of the other peer and at least meet the following conditions:

1. The crypto map entry must contain a compatible cryptographic access list (such as a mirror image access list).

2. Encryption map entries on both sides must determine the peer address of the other party (unless the peer is using a dynamic encryption map).

3. Encryption map entries must have at least one identical transformation.

4. Only one set of cryptographic maps is applied to a single interface. The crypto map set contains IPSec/IKE, or a combination of IPSec/manual entries. If multiple crypto map entries are created for a given interface, the map entries are ordered using the seq-num Parameter of the map entries; the lower the seq-num value, the higher the priority.

Multiple crypto map entries must be created for an interface if one of the following conditions exists:

1. If different data flows on this interface will be handled by different IPSec peers.

2. If you want to apply different IPSec security to different types of communication (to the same or different peers); Communications are both authenticated and encrypted. In this case, the different types of communication should be defined in two different access lists, and a

separate crypto map entry must be created for each crypto access list.

For the usage of dynamic crypto map, please refer to the usage guide of crypto dynamic-map.

【Configuration Example]】1: Manual IPSec SA minimum configuration.

```
AC-FS(config)# crypto map mymap 3 IPSec-manual
AC-FS(config-crypto-map)# set peer 2.2.2.2
AC-FS(config-crypto-map)# set session-key inbound esp 301 cipher abcdef1234567890 AC-
FS(config-crypto-map)# set sesession-key outbound esp 300 cipher abcdef1234567890 AC-
FS(config-crypto-map)# set transform-set myset
AC-FS(config-crypto-map)# match address 101
```

2: The minimum configuration of the IPSec SA negotiated by IKE.

```
AC-FS(config)# crypto map mymap 4 IPSec-isakmp AC-
FS(config-crypto-map)# set peer 2.2.2.2 AC-
FS(config-crypto-map)# set transform-set myset
AC-FS(config-crypto-map)# match address 101
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.27 Crypto map (interface IPSec)

Apply a predefined set of cryptographic maps to the interface.

crypto map map-name

Disassociates the crypto map collection from an interface.

no crypto map [map-name]

【Parameter Description】

Parameter	Description

map-name	Encrypt the mapping name.

【Default Configuration】 No encryption map is applied to the interface.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 Use this command to apply a crypto map collection to an interface. To provide IPSec cryptographic protection of data on an interface, a set of cryptographic maps must be applied to the interface. For an interface, only one crypto map collection can be associated. If multiple crypto-map entries have the same map-name and different seq-nums, they are in the same set and are applied to the same interface, the crypto-map entry with the smaller Seq-num has higher priority, and the first make a judgment.

A crypto map set can only be configured on one interface.

【Configuration Example]】 1: Apply the encrypted map named mymap to interface s0.

```
AC-FS(config)# interface  serial  0
AC-FS(config-if)# crypto map mymap
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

17.28crypto map local-address

Specifies a fixed local address for IPSec.

crypto map map-name local-address interface-type interface-number

Unassign IPSec local address.

no crypto map map-name local-address

【Parameter Description】

Parameter	Description
map-name	IPSec Encryption map name.
interface-type	Interface type used as the IPSec local address.
interface-number	Interface number used as the IPSec local address.

【Default Configuration】 The interface from which IPSec data is sent will take the address of the current interface as the IPSec local address.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】If an encryption map is applied to multiple interfaces and this command is not used, RGOS will create its own IPSec security association on each interface for the same remote peer and the same traffic. The egress IP is used as the local address. After using this command to specify the local address, the same encryption map is applied to several interfaces, only one IPSec SA will be created, and one SA will be used for communication uniformly. If a device has multiple interfaces that allow IPSec communication, in order to facilitate management, you can use this command to specify the IPSec local address, so that RGOS will use a fixed single address to communicate with external routes.

In general, we recommend using the loopback address as the IPSec local address.

【Configuration Example]】1: Specify the Loopback0 address as the local IPSec address.

```
AC-FS(config)# crypto map mymap local-address loopback 0
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.29 debug crypto engine

Turn on the debugging switch for the working state of the encryption card.

debug crypto engine

Turn off the debugging switch for the working state of the encryption card.

no debug crypto engine

【Parameter Description】-

【Default Configuration】 Turn off the debugging switch.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Turn on the debugging switch of the working state of the encryption card.

```
AC-FS# debug crypto engine
```

2: Turn off the debugging switch of the working state of the encryption card.

```
AC-FS# no debug crypto engine
```

【Debug information】-

【Prompt Information】-

【Platform Description】 -

17.30debug crypto IPSec

Enable the debugging of IPSEC packet forwarding.

debug crypto IPSec

Disable the IPSEC packet forwarding debugging switch.

no debug crypto IPSec

【Parameter Description】-

【Default Configuration】 Turn off the debugging switch.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Enable the debugging of IPSEC packet forwarding.

```
AC-FS# debug crypto IPSec
```

2: Disable the IPSEC packet forwarding debugging switch.

```
AC-FS# no debug crypto IPSec
```

【Debugging information】1: Packet encryption and decryption events.

Debug information	can not find sa 727130249, vrf 0
Information interpretation	Security association with SPI 727130249 was not found in vrf 0.
Causes	When a packet is received and needs to be decrypted, IPSEC will search for the SA to decrypt according to the SPI and other information in the packet. If it is not found, the above information will be prompted. This situation often occurs under the 3G link. Because the link is unstable, it is easy to cause inconsistency between the two ends of IPSEC, that is, one end exists and the other does not exist.
Deal with suggestions	If this situation occurs frequently, the IPSEC keep-alive mechanism DPD needs to be configured.
Debug information	packet need encrypto but not!
Information interpretation	IPSEC received messages that should be encrypted without encryption.
Causes	Most because there is a IPSEC configuration at one end and the other end, when the IPSEC end receives the message, the report is found Text are discarded without encryption.
Deal with suggestions	Check the configuration at both ends.

【Prompt Information】-

【Platform Description】 -

17.31 debug crypto isakmp

Turn on the IKE debug switch.

debug crypto isakmp

Turn off the IKE debug switch.

no debug crypto isakmp

【Parameter Description】-

【Default Configuration】 Turn off the debugging switch.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Enable IKE debugging.

```
AC-FS# debug crypto isakmp
```

2: Turn off the IKE debugging switch.

```
AC-FS# no debug crypto isakmp
```

【Debug information】 1: Protocol message event.

Debug information	received packet from 9.9.9.1, (R) MM_SR1_WI2, MM_KEY_EXCH
Information interpretation	Receiving the IKE negotiation message from 9.9.9.1, the negotiation mode is the main mode, and we have sent the first message at the time we receive the message SR1, which is awaiting the initiator's second message, WI2.
Causes	Each function processing the received message during the IKE negotiation process has similar printing.
Deal with suggestions	-

2: One-stage policy matching event.

Debug information	(main mode)process in I1:no fit sa attribute was accepted!
Information interpretation	When the receiver processes the first negotiation message I1 of the initiator, no appropriate one-stage policy configuration was found.
Causes	The one-stage policies configured by the receiver and the initiator are inconsistent.
Deal with suggestions	Check that the IKE policy configuration for both devices is consistent.

3: Negotiate authentication events.

Debug information	Check main mode hash payload fail!
Information interpretation	Main mode IKE negotiation authentication failed.
Causes	The final stage of the IKE negotiation requires verifying the identity of the other party, and in the pre-sharing authentication method, both parties need to use the configured pre-sharing Enjoy the key to authenticate each other.
Deal with suggestions	Confirm the pre-shared key configuration.

【Prompt Information】 -

【Platform Description】 -

17.32 encryption (IKE policy)

Specifies the encryption algorithm for the IKE policy.

encryption { des | 3des | aes-128 | aes-192 | aes-256 }

Restore the default encryption algorithm.

no encryption

【Parameter Description】

Parameter	Description
des	Specifies the 56-bit DES-CBC as the encryption algorithm.
3des	Specifies the 168-bit 3DES-CBC as the encryption algorithm.
aes-128	An AES with a key length of 128 bits is specified as the encryption algorithm.
aes-192	An AES with a key length of 192 bits is specified as the encryption algorithm.
aes-256	Specifying an AES with a key length of 256 bits is used as the encryption algorithm.

【Default Configuration】 56-bit DES-CBC encryption algorithm.

【Command Mode】 IKE policy configuration mode

【Default Level】 14

【Usage Guide】 The data encryption algorithm specified by this command is used for data encryption of IKE SA, which is different from the encryption algorithm of IPSec SA.

【Configuration Example]】1: Specify the encryption algorithm of the IKE policy as DES.

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.33group (IKE policy)

Specifies the Diffie-Hellman group ID in the IKE policy.

group { 1 | 2 }

Restore the Diffie-Hellman group ID to default.

no group

【Parameter Description】

Parameter	Description
1	Specifies the 768-bit Diffie-Hellman group.
2	Specify the 1,024-bit Diffie-Hellman group.

【Default Configuration】 768-bit Diffie-Hellman group (group 1).

【Command Mode】 IKE policy configuration mode

【Default Level】 14

【Usage Guide】 Use this command to specify the Diffie-Hellman group used in the IKE policy.

【Configuration Example]】1: Specify the Diffie-Hellman group of the IKE policy to be 1024 bits.

```
AC-FS(config)# crypto  isakmp policy 10
AC-FS(isakmp-policy)# group 2
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.34hash (IKE policy)

Specifies the HASH algorithm in the IKE policy.

hash { sha | md5 }

Restore the hash algorithm to the default value.

no hash

【Parameter Description】

Parameter	Description
sha	Specify the SHA-1 (HMAC variant) as the HASH algorithm.
md5	Specify the MD5 (HMAC variant) as the HASH algorithm.

【Default Configuration】 The default HASH algorithm is sha.

【Command Mode】 IKE policy configuration mode

【Default Level】 14

【Usage Guide】 Use this command to specify the HASH algorithm used in the IKE policy.

【Configuration Example】1: Specify the HASH algorithm as md5.

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.35lifetime (IKE policy)

Specifies the lifetime of the IKE SA.

lifetime seconds

Restore the lifetime to the default value.

no lifetime

【Parameter Description】

Parameter	Description
seconds	The IKE lifecycle value (seconds).Use inteinteger between 60 and 86400 seconds.

【Default Configuration】 86400 seconds (1 day).

【Command Mode】 IKE policy configuration mode

【Default Level】 14

【Usage Guide】 Use this command to specify the life cycle of IKE SA. When IKE starts negotiating, the first thing it does is agree on security parameters for its conversation. These consistent parameters are referenced by the IKE SA on each peer and retained on each peer until the IKE SA lifetime expires.

A new SA must be negotiated before the current SA expires.

Since the IPSec SA negotiation is based on the IKE SA, to save the time of negotiating the IPSec SA, you should configure a longer IKE SA lifetime. However, the probability of being cracked is proportional to the life cycle, that is, the longer the life cycle, the greater the probability of being cracked, and the shorter the life cycle, the less likely it is to be cracked. Therefore, it is necessary to set a suitable life

cycle (eg half a day).

【Configuration Example]】1: Set the life cycle of the IKE SA to 1000 seconds.

```
AC-FS(config)# crypto  isakmp policy 10
AC-FS(isakmp-policy)# lifetime 1000
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.36 match address (IPSec)

Specifies an access list of crypto map entries.

match address access-list-number

Delete the access list in the crypto map entry.

no match address

【Parameter Description】

Parameter	Description
access-list-number	Access the list number (100-199,2000-2699,2900-3899), encryption mapping only IP Extended access list.

【Default Configuration】 The encryption map entry has no specified access list.

【Command Mode】Encryption mapping configuration mode

【Default Level】 14

【Usage Guide】 This command specifies the access list of encrypted map entries. Crypto map entries use access lists to determine which data should be protected by IPSec.

The access list specified by this command is used for both outbound and inbound communications. In the case of outbound, matching data is detected. If there is already a SA, the data will be encrypted and forwarded. If no SA is established, SA Negotiation (IKE) will be triggered. In the case of entering the station, the matching data is detected, if it is encrypted data, it is decrypted, and if it is unencrypted data, it is directly discarded.

【Configuration Example]】1: Associate access list 101 on the encrypted map named mymap.

```
AC-FS(config)# crypto map mymap 4 IPSec-isakmp
AC-FS(config-crypto-map)# match address 101
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.37 match any

Specify the stream of interest as the local IP address/mask (0.0.0.0/0.0.0.0) and the peer IP address/mask (0.0.0.0/0.0.0.0).

match any

Cancel the specified stream of interest as the local ip address/mask (0.0.0.0/0.0.0.0) and the peer ip address/mask (0.0.0.0/0.0.0.0).

no match any

【Parameter Description】-

【Default Configuration】 By default, the stream of interest is not the local IP address/mask (0.0.0.0/0.0.0.0) or the peer IP address/mask (0.0.0.0/0.0.0.0).

【Command Mode】Encryption mapping configuration mode

【Default Level】 14

【Usage Guide】 This command is used to specify the stream of interest in the profile encryption map set as the local IP address/mask (0.0.0.0/0.0.0.0) and the peer IP address/mask (0.0.0.0/0.0.0.0). This profile is mainly used for ipsec over gre and l2tp over ipsec.

If the profile of ipsec over gre is configured with match any, the interesting flows in the second phase of ipsec negotiation are: local ip address/mask (0.0.0.0/0.0.0.0), peer ip address/mask (0.0.0.0 /0.0.0.0.

【Configuration Example]】1: On the profile encryption map named test.

```
AC-FS(config)#crypto ipsec profile test
AC-FS(config-crypto-profile)#match any
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.38mode (IPSec)

Change the mode of the encrypted transform collection.

mode { tunnel | transport }

Restore default mode.

no mode

【Parameter Description】

Parameter	Description
tunnel	Specifies the pattern for the transformation set: Channel mode.
transport	Specifies the mode for the transformation set: Transport mode.

【Default Configuration】 Channel mode.

【Command Mode】Encryption transformation configuration mode

【Default Level】 14

【Usage Guide】 The mode setting is only useful for those communications where both the source and destination addresses are IPSec

peers; it is not useful for other communications (all other communications take place in tunnel mode).

If the communication to be protected has the same IP address as the IPSec peer, i.e. those source and destination addresses are IPSec peers, and a transport mode is specified, then during negotiation, the device will request a transport mode, but both The transport mode can in turn accept tunnel mode. If the channel mode is specified, the device will request the channel mode and only accept the channel mode.

【Configuration Example】 1: Specify the mode of the transform set as channel mode.

```
AC-FS(config)#
AC-FS(config)#crypto ipsec transform-set myset
AC-FS(cfg-crypto-trans)#mode tunnel AC-FS(cfg-
crypto-trans)#mode transport AC-FS(cfg-crypto-
trans)#
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

17.39 reverse-route

Reverse route injection function, after configuration, after tunnel negotiation is completed, the IPSec module will automatically add a static route, pointing to the opposite end of the tunnel, or specifying an ip. Enable directional route injection.

reverse-route [remote-peer ip-address] [distance]

Remove reverse route injection feature.

no reverse-route [remote-peer ip-address] [distance]

【Parameter Description】

Parameter	Description
ip-address	Specify the next hop address, optional.
distance	Next jump distance.Range of values: 1 to 255.

【Default Configuration】 It is not enabled by default.

【Command Mode】Encryption mapping configuration mode

【Default Level】 14

【Usage Guide】 The added route can be seen by using show ip route.

The process of adding and removing can be seen through the debug crypto IPSec command.

【Configuration Example]】 1: Specify the mode of the transform set as channel mode.

```
AC-FS(config)# crypto  map mymap 5 ipsec-isakmp
AC-FS(config-crypto-map)# reverse-route
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】

17.40 self-identity

Specifies the form that the local identity takes.

self-identity { address | fqdn fqdn | user-fqdn user-fqdn }

Restore the default ontology identity form.

no self-identity

【Parameter Description】

Parameter	Description
address	Local, IP, Address.
fqdn	Local-set domain name.
user-fqdn	Local settings for the users and domain names.

【Default Configuration】 Local IP address.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】It is mainly used to complete the setting of the identity identifier in the negotiation initiated in the active mode. The local identity can be specified by the domain name, or the local identity can be specified by the address.

【Configuration Example]】1: The following example completes the identity setting:

```
AC-FS(config)# self-identity
AC-FS(config)# self-identity
 fqdn www.vpdn.com

address
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.41set autoup

Set up the tunnel to connect automatically.

set autoup

reset.

no set autoup

【Parameter Description】

Parameter	Description
access-list-number	Access the list number (100-199,2000-2699,2900-3899), encryption mapping only IP Extended access list.

【Default Configuration】 Not enabled.

【Command Mode】Encryption mapping configuration mode

【Default Level】 14

【Usage Guide】 It can avoid packet loss caused by negotiated tunnel. It is sensitive to data transmission and needs to be used in scenarios where the tunnel needs to be up at any time.

【Configuration Example】1: Complete the setting of working mode (active mode).

```
AC-FS(config)# crypto map mymap 10  IPSec-isakmp
AC-FS(config-crypto-map)# set autoup
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.42set exchange-mode

Set the working mode used in the first phase of IKE negotiation between peers.

set exchange-mode { main | aggressive }

Restore default working mode.

no set exchange-mode

【Parameter Description】

Parameter	Description
main	holotype.
aggressive	Positive mode.

【Default Configuration】 Main mode.

【Command Mode】Encryption mapping configuration mode

【Default Level】 14

【Usage Guide】 The IKE negotiation process is divided into two stages:

The first phase - implements the establishment of a secure, authenticated channel between two ISAKMP entities for communication. The modes used in this phase are Main Mode and Aggressive Mode.

The second stage - mainly negotiating the Security Association (SA) representing the service

In the first stage, there are two working modes. According to their respective advantages and disadvantages, in the default case, we use the main mode, but when the IP address is not fixed, the aggressive mode can be used.

【Configuration Example】1: Setting of working mode (active mode).

```
AC-FS(config)# crypto map mymap 10 IPSec-isakmp
AC-FS(config-crypto-map)# set exchange-mode aggressive
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.43set isakmp-policy

Specifies the negotiation policy for the corresponding map.

set isakmp-policy number

Do not specify policy negotiation.

no set isakmp-policy

【Parameter Description】

Parameter	Description

number	The negotiation policy serial number as specified

【Default Configuration】 Negotiate without specifying a policy

【Command Mode】Encryption mapping configuration mode

【Default Level】 14

【Usage Guide】In aggressive mode, the branch only sends the policy with the highest priority to the headquarters for negotiation by default. Therefore, if the same branch negotiates with multiple headquarters in aggressive mode, all the policies with the highest priority of the headquarters are required to be negotiated with the branch. Consistently, this requirement reduces device compatibility. Using this command, you can specify the corresponding map to use the configured policy for negotiation, and it is not necessary that the policy with the highest priority in the headquarters is the same. This command only takes effect under static map, dynamic map cannot be configured.

【Configuration Example]】1: Specify the static map AC-FS to use the policy with serial number 2 for negotiation.

```
11.x_site1(config)#crypto map AC-FS 100 ipsec-isakmp
11.x_site1(config-crypto-map)#set isakmp-policy 2
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.44 set local (IPSec)

Specifies the local ip in the crypto map entry.

set local ip-address

Remove the remote peer in the crypto map entry.

no set local ip-address

【Parameter Description】

Parameter	Description
ip-address	The IP address used in this segment.

【Default Configuration】Do not specify any remote peer.

【Command Mode】Encryption mapping configuration mode

【Default Level】 14

【Usage Guide】 It is used to set the ip address used for negotiation in this section. If there is no configuration, use the primary address of the interface to negotiate. Use the specified address after configuration.

【Configuration Example]】1: Encryption map mymap specifies a remote peer (2.2.2.2).

```
AC-FS(config)# crypto  map mymap 5 IPSec-isakmp
AC-FS(config-crypto-map)# set local 2.2.2.2
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.45set mtu

Set IPSec pre-fragmentation mode (tunnel mode is valid).

set mtu length

Do not use pre-sharding mode.

no set mtu

【Parameter Description】

Parameter	Description

length	Package packet slice size, ranging from 512 to 1500.

【Default Configuration】 Do not use pre-sharding mode.

【Command Mode】Encryption mapping configuration mode

【Default Level】 14

【Usage Guide】 Specify the IPSec tunnel encapsulation to use pre-fragmentation mode.

【Configuration Example]】1: The encrypted map mymap specifies the pre-sharding mode.

```
AC-FS(config)# crypto  map mymap 5 IPSec-isakmp
AC-FS(config-crypto-map)# set mtu 1000
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.46 set peer (IPSec)

Specifies the remote peer in the crypto map entry.

set peer { hostname | ip-address }

Remove the remote peer in the crypto map entry.

no set peer { hostname | ip-address }

【Parameter Description】

Parameter	Description
ip-address	The IP address of the remote peer body.
hostname	Host name of the remote peer.

【Default Configuration】Do not specify any remote peer.

【Command Mode】Encryption mapping configuration mode

【Default Level】 14

【Usage Guide】A remote peer must be specified for all cryptomaps used.

When there are multiple certificate chains locally, specify the certificate chain according to each peer, and use the peer certificate chain ca certificate to verify if the local certificate chain is not specified. Use the default certificate chain ca certificate verification when the peer certificate chain is not specified.

【Configuration Example]】1: Encryption map mymap specifies a remote peer (2.2.2.2).

```
AC-FS(config)# crypto  map mymap 5 IPSec-isakmp
AC-FS(config-crypto-map)# set peer 2.2.2.2
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.47set peer-identical

Specifies that multiple aces use the same remote peer for phase 2 negotiation.

set peer-identical

Delete specifies that multiple aces use the same remote peer for phase 2 negotiation.

no set peer-identical

【Parameter Description】-

【Default Configuration】 The same remote peer is used when multiple ace phase 2 negotiation is not specified.

【Command Mode】Encryption mapping configuration mode

【Default Level】 14

【Usage Guide】When multiple aces are configured under one acl, and multiple remote peers are configured at the same time, this command must be configured to ensure that all ace negotiation is performed with the same peer.

【Configuration Example]】1: Encryption map mymap specifies that ace uses the same remote peer.

```
AC-FS(config)# crypto  map mymap 5 IPSec-isakmp
AC-FS(config-crypto-map)# set peer-identical
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.48 set peer-preempt

Specifies that the high-priority remote peer initiates preemption.

set peer-preempt

Delete the specified high-priority remote peer to initiate preemption.

no set peer-preempt

【Parameter Description】-

【Default Configuration】 Do not specify a high-priority remote peer to initiate preemption.

【Command Mode】Encryption mapping configuration mode

【Default Level】 14

【Usage Guide】When multiple remote peers are configured, use the peer with higher priority for negotiation.

An encrypted map map can be configured with multiple remote peers. The priority configured first is higher, and the peer with the higher

priority is used for negotiation. When the tunnel is disconnected, it switches to a peer for negotiation. If the peer with high priority can initiate negotiation, use high priority for negotiation and forwarding, and disconnect the tunnel negotiation with low priority, this command must be configured

【Configuration Example]】1: Encryption map mymap The remote peer with the specified priority initiates preemption.

```
AC-FS(config)# crypto  map mymap 5 IPSec-isakmp
AC-FS(config-crypto-map)# set peer-preempt
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.49 set pfs (IPSec)

Specifies that the IPSec tunnel encapsulation uses the Diffie-Hellman group ID.

set pfs { group1 | group2 }

Tunnel encapsulation does not use Diffie-Hellman group identity.

no set pfs

【Parameter Description】

Parameter	Description
group1	768 bits.
group2	1024 bits.

【Default Configuration】 Diffie-Hellman group is not used.

【Command Mode】Encryption mapping configuration mode

【Default Level】 14

【Usage Guide】Specify the Diffie-Hellman group identifier for IPSec tunnel encapsulation.

【Configuration Example]】1: The encrypted map mymap specifies 1024-bit Diffie-Hellman.

```
AC-FS(config)# crypto  map mymap 5 IPSec-isakmp
AC-FS(config-crypto-map)# set pfs group2
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.50set security-association lifetime

Replaces the global lifetime of a crypto map for IPSec SA negotiation.

set security-association lifetime { seconds seconds | kilobytes kilobytes] }

Restores the default value of the global lifetime of the crypto map for IPSec SA negotiation.

no set security-association lifetime { seconds | kilobytes }

【Parameter Description】

Parameter	Description
seconds seconds	Security Alliance Timeout Time (seconds).Range ranged from 120 seconds to 86,400 seconds.
kilobytes kilobytes	Timeout traffic for the security alliance (in thousand bytes).The range is 2560KB to 536870912KB.

【Default Configuration】 The security association of the cryptographic map is negotiated according to the global lifetime value.

【Command Mode】Encryption mapping configuration mode

【Default Level】 14

【Usage Guide】 This command is only useful for using IKE to establish the encryption map of IPSec SA. The cryptographic map of the

manually created SA does not have this command.

By default, all IPSec SAs use the global lifetime value for negotiation. If a target address needs to be negotiated with a lifetime different from the global lifetime value, you can negotiate with the target address in the encryption Use this command in a map entry to modify the lifetime value.

Modifying the lifetime value with this command only changes the lifetime value of a specific mapping for IPSec SA negotiation, and does not affect the global lifetime value.

【Configuration Example]】1: Change the life cycle of the encrypted map mymap entry 5 to 2500 seconds.

```
AC-FS(config)# crypto  map mymap 5 IPSec-isakmp
AC-FS(config-crypto-map)# set security-association lifetime  seconds 2500
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.51set session-key

Set the security parameter indices (SPIs) and passwords of the relevant algorithms for outbound and inbound protected communications.

set session-key { inbound | outbound } ah spi hex-key-data

set session-key { inbound | outbound } esp spi { cipher hex-key-data | authenticator hex-key-data }

Removed security parameter indices (SPIs) and passwords for related algorithms.

no set session-key { inbound | outbound } ah no set session-key { inbound | outbound } esp

【Parameter Description】

Parameter	Description
spi	Security Parameter index.
hex-key-data	It is a 16-decimal password.

【Default Configuration】 Do not specify the security parameter index and password of any related algorithm.

【Command Mode】Encryption mapping configuration mode

【Default Level】 14

【Usage Guide】 It is used to create SA manually, only used in IPSec-manual.

【Configuration Example]】1: Encryption map mymap specifies esp encapsulation and decapsulation password abcdef1234567890.

```
AC-FS(config)# crypto  map mymap 5 ipsec-manual
AC-FS(config-crypto-map)# set session-key inbound esp 301 cipher abcdef1234567890
AC-FS(config-crypto-map)# set session-key outbound esp 300 cipher abcdef1234567890
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.52 set transform-set

Set transform-set transform-set-name1 [transform-set-name2] [transform-set-name3] [transform-set-name4] [transform-set-name5] [transform-set-name6]

Crypto map entries do not use transform sets.

no set pfs

【Parameter Description】

Parameter	Description
transform-set-name1 [transform-set-name2] [transform-set-name3] [transform-set-name4] [transform-set-name5] [transform-set-name6]	Transform the set name, and you can specify up to six transform sets for the encrypted mapping entries.

【Default Configuration】 No transformation set is specified.

【Command Mode】Encryption mapping configuration mode

【Default Level】 14

【Usage Guide】The transformation set is a necessary condition for the successful establishment of a security association. Configuring any crypto map requires specifying a transform set with this command.

【Configuration Example]】1: Specify the transformation set of the encrypted map entry as myset.

```
AC-FS(config)# crypto IPSec transform-set myset esp-des esp-sha-hmac AC-
FS(config)# crypto  map mymap 5 IPSec-isakmp
AC-FS(config-crypto-map)# set transform-set myset
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.53 show crypto dynamic-map (IPSec)

View information about dynamic crypto maps.

show crypto dynamic-map [map-name]

【Parameter Description】

Parameter	Description
map-name	The name of the encryption map.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to view the PIM interface on the device, the PIM neighbors on the interface, the interval for sending

Hello messages, and the DR address.

【Configuration Example]】1: View the information of all dynamic encryption maps

```
AC-FS# show crypto dynamic-map
        Crypto Map Template "mydmap" 1
No matching address list set.
Security association lifetime: 4608000 kilobytes/3600 seconds(id=34)
PFS (Y/N): N
Transform sets = {  }
```

【Prompt Information】-

【Platform Description】 -

17.54 show crypto IPSec sa

View specific information about currently active IPSec SAs.

show crypto IPSec sa

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: View the specific information of the currently active IPSec SA.

```
Interface: GigabitEthernet 1/0/0

        Crypto map tag:mymap, local addr 2.2.2.3

        media mtu 1500

        sub_map type:static, seqno:7, id=0

        local  ident (addr/mask/prot/port): (2.2.2.3/0.0.0.0/0/0))

        remote  ident (addr/mask/prot/port): (2.2.2.2/0.0.0.0/0/0))

        PERMIT

        #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0

        #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0

        #send errors 0, #recv errors 0

        Inbound esp sas:

             spi:0x79b8e4bb (2042160315)

              transform: esp-3des

              in use settings={Tunnel,}

              crypto map mymap 7

              sa timing: remaining key lifetime (k/sec): (4607000/3505)

              IV size: 8 bytes

              max reply windows size: 0

              Replay detection support:Y



        Outbound esp sas:

             spi:0x293b8b55 (691768149)

              transform: esp-3des

              in use settings={Tunnel,}

              crypto map mymap 7

              sa timing: remaining key lifetime (k/sec): (4607000/3505)

              IV size: 8 bytes

              max reply windows size: 0

              Replay detection support:Y
```

【Prompt Information】-

【Platform Description】 -

17.55 show crypto IPSec transform-set

View information about the transform set of the device configuration.

show crypto IPSec transform-set

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: View the information about the transform set of the device configuration.

```
AC-FS# show crypto IPSec transform-set
transform set myset3: { esp-des,}
        will negotiate = {Tunnel,}
```

【Prompt Information】-

【Platform Description】 -

17.56 show crypto isakmp policy

View the IKE policy information configured on the device.

show crypto isakmp policy

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: View the IKE policy information configured by the device.

```
AC-FS# show crypto isakmp policy
Protection suite of priority 9
encryption algorithm: 3DES - Data Encryption Standard (56 bit keys).
hash algorithm:         Message Digest 5
authentication method: Pre-Shared Key
Diffie-Hellman group: #2 (1024 bit)
lifetime:               1000 seconds
Protection suite of priority 10
encryption algorithm: DES - Data Encryption Standard (56 bit keys).
hash algorithm:         Message Digest 5
authentication method: Pre-Shared Key
Diffie-Hellman group: #2 (1024 bit)
lifetime:               1000 seconds
Default protection suite
encryption algorithm: DES - Data Encryption Standard (56 bit keys).
hash algorithm:         Secure Hash Standard
authentication method: Pre-Shared Key
Diffie-Hellman group:  #1 (768 bit)
lifetime:               86400seconds
```

【Prompt Information】-

【Platform Description】 -

17.57show crypto isakmp sa

View the IKE SAs currently active on the device.

show crypto isakmp sa

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: View the current active IKE SAs on the device.

```
AC-FS# show crypto isakmp sa
destination    source     state      conn-id   lifetime(second)
 1.1.1.1.....1.1.1.2    IKE_IDLE  59          32254
```

【Prompt Information】-

【Platform Description】 -

17.58 show crypto log

View the login and logout logs of IPSec VPN.

show crypto log

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】View the login and logout logs of IPSec VPN.

```
AC-FS # sh cr log
Time                    RemoteName
PeerIP/Port                                    Action          Reason          Interface
Proto:(Local)ip/mask/port <--> (Peer)ip/mask/port
```

```
------------------------------------------------------------------------------
------------------------------------------------------------------------------
------------------------------------------------------------------------------
------------------------------------------------------------------------------

2014-11-15-01:07:06    3.3.3.3
3.3.3.3/500                                    logout          DEL_IPS_PKT     Gi0/1
17:3.3.3.3/32/1701<-->3.3.3.3/32/1701
2014-11-15-01:07:06    3.3.3.3
3.3.3.3/500                                     logout          DEL_ISA_PKT     Gi0/1
NULL
```

【Prompt Information】-

【Platform Description】 -

17.59 show crypto log remotename

Specify the peer name (IP, etc.) to filter and view the login and logout logs of IPSec VPN.

show crypto log remotename name

【Parameter Description】

Parameter	Description
name	Specifies the paired-end name for the display log.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】Specify the peer name (IP, etc.) to filter and view the login and logout logs of IPSec VPN.

```
11.x_site1#show crypto log remotename 61.100.1.20

total log numbers: 184
```

```
Time                    RemoteName
PeerIP/Port                                    Action          Reason          Interface
Proto:(Local)ip/mask/port <--> (Peer)ip/mask/pot

------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------
2015-10-16-03:50:14    61.100.1.20
61.100.1.20/500                                 login           NA              Gi0/2
NULL
2015-10-16-03:50:14    61.100.1.20
61.100.1.20/500                                login           NA              Gi0/2
0:1.1.1.0/24/0<-->2.2.2.0/24/0
2015-10-16-03:55:50    61.100.1.20
61.100.1.20/500                                logout          CLR_ISA_SA      Gi0/2
0:1.1.1.0/24/0<-->2.2.2.0/24/0
2015-10-16-03:56:51    61.100.1.20
61.100.1.20/500                                 logout          IDLE_TIMER      Gi0/2
NULL
Filter log numbers: 4
11.x_site1#
```

【Prompt Information】-

【Platform Description】 -

17.60 show crypto log remotename name start start_lines end end_lines

Specify the peer name (IP, etc.) to filter and view the login and logout logs of IPSec VPN, and specify the number of lines to display in the filter result.

show crypto log remotename name start start_lines end end_lines

【Parameter Description】

Parameter	Description
name	Specifies the paired-end name for the display log.
start_lines	Specifies the starting row showing the log.
end_lines	Specifies the termination row showing the log.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】】Specify the peer name (IP, etc.) to filter and view the login and logout logs of IPSec VPN, and display the specified number of lines in the filter result.

```
11.x_site1#show crypto log remotename 61.100.1.20 start 1 end 2

total log numbers: 188

Time                    RemoteName
PeerIP/Port                                    Action          Reason          Interface
Proto:(Local)ip/mask/port <--> (Peer)ip/mask/pot

------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------
2015-10-16-03:50:14    61.100.1.20
61.100.1.20/500                                 login           NA              Gi0/2
NULL
2015-10-16-03:50:14    61.100.1.20
61.100.1.20/500                                 login           NA              Gi0/2
0:1.1.1.0/24/0<-->2.2.2.0/24/0
Filter log numbers: 4
```

【Prompt Information】-

【Platform Description】 -

17.61 show crypto log start start_lines end end_lines

Specify the number of lines to view the login and logout logs of IPSec VPN.

show crypto log start start_lines end end_lines

【Parameter Description】

Parameter	Description
start_lines	Specifies the starting row showing the log.
end_lines	Specifies the termination row showing the log.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】Specify the number of lines to view the login and logout logs of IPSec VPN.

```
11.x_site1#show crypto log start 1 end 2

total log numbers: 184

Time                    RemoteName
PeerIP/Port                                    Action          Reason          Interface
Proto:(Local)ip/mask/port <--> (Peer)ip/mask/pot

------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------
2015-10-16-03:23:55    NO_NAME                                                          (null)/0
restart          IPSEC_RESTART                          NULL
2015-10-16-03:42:57    NO_NAME                                                          (null)/0
restart          IPSEC_RESTART                          NULL
11.x_site1#
```

【Prompt Information】-

【Platform Description】 -

17.62 show crypto map (IPSec)

View information about crypto maps.

show crypto map [map-name]

【Parameter Description】

Parameter	Description

map-name	The name of the encryption map.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example]】 1: View the information of all encryption maps.

```
AC-FS# show crypto map

Crypto Map:"mymap1" 1 IPSec-isakmp, (Complete)
        Extended IP access list 100
        Security association lifetime: 0 kilobytes/120 seconds(id=2)
        PFS (Y/N): N
        Transform sets = { myset3,  }

        Interfaces using crypto map mymap1:
                GigabitEthernet 1/1/0
```

【Prompt Information】 -

【Platform Description】 -

17.63 tunnel protection IPSec profile

Apply the predefined set of Profile cryptographic maps to the Tunnel interface.

tunnel protection IPSec profile [profile-name]

Disassociates the crypto map collection from an interface.

no tunnel protection IPSec profile [profile-name]

【Parameter Description】

Parameter	Description
profile-name	Profile Encryption map name.

【Default Configuration】 No encryption map is applied to the Tunnel interface.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】Use this command to apply a crypto map collection to an interface. To perform IPSec encryption protection on all packets on a tunnel interface, an encryption map set must be applied to this interface. For an interface, only one crypto map collection can be associated.

Profile map can only support applications on GRE, IPIP, and IPV6 tunnels. If it is configured on an unsupported tunnel, the configuration will fail, or if the tunnel mode is changed to a mode not supported by the profile, the map on the tunnel interface will be disabled. delete.

【Configuration Example]】1: Apply the encrypted map named profile-name to interface Tunnel 1.

```
AC-FS(config)# interface tunnel 1
AC-FS(config-if-Tunnel 1) # tunnel protection IPSec profile profile-name

2: Apply the encryption mapping named test to the interface virtual-ppp 1: AC-FS(config)#crypto ipsec profile test
AC-FS(config-crypto-profile)#exit AC-FS(config)#
AC-FS(config)#int virtual-ppp 1

AC-FS(config-if-Virtual-ppp 1)#tunnel protection ipsec profile test AC-FS(config-if-Virtual-ppp 1)#exit
AC-FS(config)#
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

18 VPDNs

18.1accept dialin

Set the tunnel working mode to accept incoming calls.

accept-dialin

Restore system default settings

no accept-dialin

【Parameter Description】-

【Default Configuration】 By default, the system does not set the tunnel working mode.

【Command Mode】 VPDN-Group interface configuration mode

【Default Level】 14

【Usage Guide】 By default, the system does not specify any tunnel working mode for VPDN-Group. The user must first set the tunnel working mode before further setting the tunnel working protocol and the bound virtual template interface. The valid settings or changes of this command will immediately cause the existing related tunnels to be actively forcibly removed.

【Configuration Example】1: Set the tunnel working mode to accept dial-in.

```
AC-FS(config)#vpdn-group 1
AC-FS(config-vpdn)#accept-dialin
AC-FS(config-vpdn-acc-in)#
```

【Verification】Use the show running-config command to check whether the tunnel working mode is to accept dial-in.

【Prompt Information】-

【Common Mistake】 The effective setting or change of this command will immediately cause the existing related tunnel to be actively forcibly removed.

【Platform Description】 -

18.2Authentication (L2TP)

Enable channel verification.

authentication

Restore system default settings

no authentication

【Parameter Description】-

【Default Configuration】 By default, the system disables the channel authentication function.

【Command Mode】 L2TP-Class interface configuration mode

【Default Level】 14

【Usage Guide】Users can enable or disable the channel verification function according to their needs.

【Configuration Example】1: Enable the channel verification function.

```
AC-FS(config)#l2tp-class 1
AC-FS(config-l2tp-class)#authentication
AC-FS(config-l2tp-class)#
```

【Verification】Use the show running-config command to check whether the channel verification function is enabled.

【Prompt Information】-

【Common Mistake】Effective changes to the tunnel verification function settings will cause the related tunnels referencing the L2TP-Class to be actively forcibly removed.

【Platform Description】 -

18.3 clear vpdn log

Clear the user log-off and log-off information saved in the log file

clear vpdn log

【Parameter Description】-

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】This command will clear the user online and offline information saved in the log file

【Configuration Example]】1: Clear the user log on and off information saved in the log file

```
AC-FS# show vpdn log
Username          IP   State Online time     Offline time
user-1                          100.1.1.2  out---------------------------------------------------------------- 2014-11-16-14:09:04
2014-11-16-14:29:26
user-2                          100.1.2.2  out     2014-11-16-15:09:05 2014-11-16-16:09:27
AC-FS# clear vpdn log AC-FS#
AC-FS# show vpdn log
%No vpdn logs. AC-FS#
```

【Prompt Information】-

【Platform Description】 First supported item 11_1_PJ5

18.4 clear vpdn tunnel

Force clear the specified tunnel.

clear vpdn tunnel [{ l2tp | pptp } [id locid] | [remote-host-name]]

【Parameter Description】

Parameter	Description
l2tp	L2TP tunnel.
pptp	PPTP tunnel.
remote-host-name	Tunnel end-to-end host name.
locid	Specify the tunnel ID delete the corresponding tunnel.

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】 This command will force clear the specified tunnel. If Parameter is not used, all existing tunnels (including PPTP and L2TP tunnels) will be forcibly cleared; if only the tunnel protocol is specified, all tunnels corresponding to the tunnel protocol will be forcibly cleared; if the host name of the tunnel peer is also specified, then Forcibly clear the tunnel whose peer host name matches the specified name in the corresponding tunnel protocol-related tunnel.

Specify the tunnel ID The ID used in the delete tunnel is the tunID information in show vpdn.

【Configuration Example】 1: Clear all existing L2TP tunnels.

```
AC-FS# show vpdn
L2TP Tunnel and Session Information Total tunnels 1 sessions 1
LocID RemID Remote Name State  Remote Address  Port  Sessions L2TP Class/
VPDN Group
1     1     BLIZZARD   est.....192.168.12.213  1701  1  1
LocID       RemID       TunID       Username,   Intf/
State  Last Chg                          Vcid, Circuit
1           1           1           ms,Vi1               est
00:46:30
%No  active PPTP  tunnels AC-
FS# clear vpdn tunnel l2tp AC-
FS#
%UPDOWN: Line protocol on Interface Virtual-Access1, changed state to down
%CHANGED: Interface Virtual-Access1, changed state to administratively down AC-
FS# show vpdn
%No active L2TP tunnels
%No active PPTP tunnels AC-
FS#
```

【Prompt Information】 -

【Platform Description】 -

18.5encapsulation (L2TP)

Sets the data encapsulation mode of the tunnel.

encapsulation l2tpv2

【Parameter Description】

Parameter	Description
l2tpv2	L2TP set by the RFC 2661 specification to transmit tunnel data.

【Default Configuration】 By default, the system does not set the data encapsulation mode of the tunnel.

【Command Mode】 Pseudowire-Class interface configuration mode

【Default Level】 14

【Usage Guide】 On the pseudowire-class interface, you must first set the tunnel data encapsulation mode before you can further set the tunnel data transmission Parameter

【Configuration Example】1: Set the tunnel data encapsulation mode to l2tpv2.

```
AC-FS(config)# AC-
FS(config)#pseudowire-class 1
AC-FS(config-pw-class)#encapsulation l2tpv2
AC-FS(config-pw-class)#
```

【Verification】Use the show running-config command to view the data encapsulation mode of the tunnel.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

18.6 force-local-chap

Force PPP to perform complete authentication again. When the Client triggers the LAC to start dialing, the LAC will proxy the LNS to authenticate the Client. This command is used to re-authenticate the Client after the L2TP tunnel is established. This command is only

valid on LNS.

force-local-chap

Restore system default settings

no force-local-chap

【Parameter Description】-

【Default Configuration】 By default, the LNS does not need to authenticate the Clinet.

【Command Mode】 VPDN-Group interface configuration mode

【Default Level】 14

【Usage Guide】 This command can be configured only after vpdn enable is configured

【Configuration Example】1: Set up tunnel re-authentication PPP LCP.

```
AC-FS(config-vpdn)# force-local-chap
AC-FS(config-vpdn)#
```

【Verification】Use the show running-config command to check whether the Clinet is authenticated.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

18.7 force-local-lcp

Force PPP to perform complete authentication again. When the Client triggers the LAC to start dialing, the LAC will proxy the LNS to authenticate the Client. This command is used to re-negotiate the Client after the L2TP tunnel is established. This command is only valid on LNS.

force-local-lcp

Restore system default settings

no force-local-lcp

【Parameter Description】-

【Default Configuration】 By default, LNS does not need to perform lcp negotiation with Clinet.

【Command Mode】 VPDN-Group interface configuration mode

【Default Level】 14

【Usage Guide】 This command can be configured only after vpdn enable is configured

【Configuration Example】1: Set up tunnel re-authentication PPP LCP.

```
AC-FS(config-vpdn)# force-local-lcp
AC-FS(config-vpdn)#
```

【Verification】Use the show running-config command to check whether the Clinet is negotiated.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

18.8 hello

This command sets the sending interval of Hello messages sent to implement L2TP channel Keepalive.

hello interval

Restore system default settings.

no hello

【Parameter Description】

Parameter	Description

interval	The Hello message sending interval is in seconds with a value range of 1-1000.

【Default Configuration】 By default, the interval for sending Hello messages is 60 seconds.

【Command Mode】 L2TP-Class interface configuration mode

【Default Level】 14

【Usage Guide】Users can set the Hello message sending interval according to the network environment to detect whether the L2TP channel is still available. If the network is stable and reliable, you can set the Hello message sending interval to a larger value.

【Configuration Example]】1: Set the Hello message sending interval to 120 seconds.

```
AC-FS(config-l2tp-class)# hello 120
AC-FS(config-l2tp-class)#
```

【Verification】Use the show running-config command to view the sending interval of the sent Hello message

【Prompt Information】

【Common Mistake】 Any effective change to the Hello sending interval setting will cause the corresponding existing L2TP tunnel to be actively forcibly removed.

【Platform Description】 -

18.9 hostname (L2TP)

Set the L2TP tunnel local end host name.

hostname local-hostname-string

Restore system default settings

no hostname

【Parameter Description】

Parameter	Description
local-hostname-string	Local-end host name of the tunnel.

【Default Configuration】 By default, the system uses the name of the router as the host name of the local end of the tunnel.

【Command Mode】 L2TP-Class interface configuration mode

【Default Level】 14

【Usage Guide】 Users can set the local host name of the tunnel as required for tunnel identification. Any valid change to the hostname on the local end of the tunnel will cause the existing corresponding L2TP tunnel to be forcibly removed

【Configuration Example]】1: The host name of the local end of the tunnel will be set to "LAC".

```
AC-FS(config-l2tp-class)# hostname LAC
AC-FS(config-l2tp-class)#
```

【Verification】Use the show running-config command to view the host name of the local end of the tunnel

【Prompt Information】

【Common Mistake】-

【Platform Description】 -

18.10 ip dfbit set

It is forbidden for tunnel data to be sent in fragments.

ip dfbit set

restore system defaults

no ip dfbit set

【Parameter Description】-

【Default Configuration】 By default, the system allows tunnel data to be sent in fragments.

【Command Mode】 Pseudowire-Class interface configuration mode

【Default Level】 14

【Usage Guide】 Users can set whether to allow tunnel data to be sent in fragments according to their needs. Any valid changes to the settings of the tunnel data fragment sending function will be immediately reflected in the tunnel data transmission, but will not cause the corresponding L2TP tunnel to be forcibly removed

【Configuration Example]】1: Forbid the tunnel data to be sent in fragments.

```
AC-FS(config-pw-class)# ip dfbit set
AC-FS(config-pw-class)#
```

【Verification】Use the show running-config command to check whether the tunnel data is prohibited from being sent by fragments

【Prompt Information】

【Common Mistake】

【Platform Description】 -

18.11 ip local interface

Set the local (source) interface used by the tunnel.

ip local interface interface-name

Restore system default settings

no ip local interface interface-name

【Parameter Description】

Parameter	Description
interface-name	Local interface name.

【Default Configuration】 By default, the local (source) interface used by the tunnel is not specified.

【Command Mode】 Pseudowire-Class interface configuration mode

【Default Level】 14

【Usage Guide】 Users can specify the network interface on the router as the local (source) interface of the tunnel. Any valid changes to the local (source) interface settings of the tunnel will cause the corresponding L2TP tunnel to be actively forcibly removed

【Configuration Example】1: Set the local (source) interface of the tunnel to Serial 0.

```
AC-FS(config-pw-class)# ip local interface serial 0
AC-FS(config-pw-class)#
```

【Verification】Use the show running-config command to view the local (source) interface used by the tunnel

【Prompt Information】

【Common Mistake】

【Platform Description】 -

18.12 ip precedence

Set the IP header priority field of the payload tunnel.

ip precedence { precedence-value | critical | flash | flash-override | immediate | internet | network | priority | routine }

Restore system default settings.

no ip precedence

【Parameter Description】

Parameter	Description
precedence-value	Value of the priority domain, with values that range from 0 to 7.
critical	The priority domain has a value of 5.
flash	The value of the priority domain is 3.
flash-override	The priority domain has a value of 4.
immediate	The priority domain has a value of 2.
internet	The priority domain has a value of 6.
network	The priority domain value is 7.
priority	The priority domain has a value of 1.
routine	The value of the priority domain is 0.

【Default Configuration】 By default, the system sets the IP header priority field value of the payload tunnel to zero, that is, routine.

【Command Mode】 VPDN-Group interface configuration mode

【Default Level】 14

【Usage Guide】 If the user needs to set the priority of the tunnel data, this command can be used. The valid settings of this command will immediately affect the tunnel data transmission, but will not cause the related tunnel to be actively forcibly torn down.

【Configuration Example】1: Set the priority of tunnel data to 7.

```
AC-FS(config-vpdn)# ip precedence 7
AC-FS(config-vpdn)#
```

【Verification】Use the show running-config command to view the IP header priority field of the load tunnel

【Prompt Information】

【Common Mistake】 This command is only valid for L2TP, not for PPTP

【Platform Description】 -

18.13 ip tos

Set the TOS (Type of Service) field of the IP header of the payload tunnel.

ip tos { tos-value | max-reliability | max-throughput | min-delay | min-monetary-cost | normal | reflect }

Restore system default settings

no ip tos

【Parameter Description】

Parameter	Description
tos-value	The value of the TOS field, ranging from 0 to 15.
max-reliability	The value of the TOS field is 2.
max-throughput	The value of the TOS field is 4.
min-delay	The value of the TOS field is 8.

min-monetary-cost	The value of the TOS field is 1.
normal	The value of the TOS field is 0.
reflect	Use the TOS of the IP packet of the tunnel payload as the TOS field of the IP header of the payload tunnel.

【Default Configuration】 By default, the TOS field of the IP header of the payload tunnel is zero.

【Command Mode】 VPDN-Group interface configuration mode

【Default Level】 14

【Usage Guide】 If the user needs to set the TOS of the tunnel data, this command can be used. The valid settings of this command will immediately affect the tunnel data transmission, but will not cause the related tunnel to be actively forcibly torn down.

【Configuration Example]】1: Set the TOS of tunnel data to min-delay.

```
AC-FS(config-vpdn)# ip tos min-delay
AC-FS(config-vpdn)#
```

【Verification】Use the show running-config command to view the TOS (Type of Service) field of the IP header of the payload tunnel

【Prompt Information】

【Common Mistake】

【Platform Description】 -

18.14 ip ttl

Sets the TTL field of the IP header of the payload tunnel data.

ip ttl ttl-value

Restore system default settings.

no ip ttl

【Parameter Description】

Parameter	Description
ttl-value	Values of the TTL domain, and the values range from 1 to 255.

【Default Configuration】 By default, the system sets the TTL field of the IP header of the payload tunnel data to 255.

【Command Mode】 Pseudowire-Class interface configuration mode

【Default Level】 14

【Usage Guide】 Users can set the TTL field of the IP header of the payload tunnel data as needed. Any valid changes to the setting of the TTL field of the IP header of the payload tunnel data will be immediately reflected in the tunnel data transmission, but will not cause the corresponding L2TP tunnel to be forcibly removed.

【Configuration Example]】 1: Set the TTL field of the IP header of the payload tunnel data to 253.

```
AC-FS(config-pw-class)# ip ttl 253
AC-FS(config-pw-class)#
```

【Verification】 Use the show running-config command to check whether there is a TTL field for setting the IP header of the payload tunnel data

【Prompt Information】

【Common Mistake】

【Platform Description】 -

18.15 l2tp ip udp checksum

This command requires the UDP packet carrying tunnel data to calculate and fill the Checksum field.

l2tp ip udp checksum

Restore system default settings.

no l2tp ip udp checksum

【Parameter Description】 -

【Default Configuration】 By default, the system requires that the Checksum field of the UDP packet carrying tunnel data be empty (ie, zero).

【Command Mode】 VPDN-Group interface configuration mode

【Default Level】 14

【Usage Guide】 The user can set whether to calculate and fill in the Checksum field for UDP packets carrying tunnel data according to their needs. You must configure protocol l2tp or protocol any before this command will be displayed.

【Configuration Example]】1: Checksum is required for UDP packets carrying tunnel data.

```
AC-FS(config)# AC-FS(config)#vpdn-
group 1 AC-FS(config-vpdn)#accept-
dialin
AC-FS(config-vpdn-acc-in)#protocol any AC-
FS(config-vpdn-acc-in)#exit AC-FS(config-
vpdn)#l2tp ip udp checksum
AC-FS(config-vpdn)#
```

【Verification】Use the show running-config command to check whether the calculation is based on the UDP packets of the load tunnel data

【Prompt Information】-

【Common Mistake】 Any valid changes to the settings of the Checksum field of the UDP packet carrying the tunnel data will be immediately reflected in the tunnel data transmission, but will not cause the corresponding L2TP tunnel to be forcibly removed.

【Platform Description】 -

18.16 l2tp tunnel authentication

Enable channel verification.

l2tp tunnel authentication

Restore system default settings.

no l2tp tunnel authentication

【Parameter Description】-

【Default Configuration】 By default, the system disables the channel authentication function.

【Command Mode】 VPDN-Group interface configuration mode

【Default Level】 14

【Usage Guide】Users can enable or disable the channel verification function according to their needs. Any effective changes to the tunnel authentication function settings will cause the related L2TP tunnels to be forcibly removed. The protocol l2tp or protocol any command must be configured before it will be displayed.

【Configuration Example】1: Enable the channel verification function.

```
AC-FS(config)# AC-FS(config)#vpdn-
group 1 AC-FS(config-vpdn)#accept-
dialin
AC-FS(config-vpdn-acc-in)#protocol any
AC-FS(config-vpdn-acc-in)#exit
AC-FS(config-vpdn)#l2tp tunnel authentication
AC-FS(config-vpdn)#
```

【Verification】Use the show running-config command to check whether the channel verification function is enabled

【Prompt Information】

【Common Mistake】

【Platform Description】 -

18.17 l2tp tunnel avp-hidden-compatible

Configuring this command indicates that the RFC2661 standard AVP Hidden parsing algorithm is compatible and supported, and the Cisco standard AVP Hidden parsing algorithm is supported by default. analysis algorithm.

l2tp tunnel avp-hidden-compatible

Restore system default settings.

no l2tp tunnel avp-hidden-compatible

【Parameter Description】-

【Default Configuration】 By default, the system adopts the Cisco standard AVP Hidden parsing algorithm.

【Command Mode】 VPDN-Group interface configuration mode

【Default Level】 14

【Usage Guide】Users can enable or disable the RFC2661 AVP Hidden parsing algorithm as needed. If you need to support two AVP Hidden resolution algorithms, you can configure multiple VPDN-Groups to achieve the goal. Configuring this command will not affect the current L2TP tunnel.

【Configuration Example]】1: The configuration is compatible with the RFC2661 standard AVP Hidden parsing function.

```
AC-FS(config-vpdn)# l2tp tunnel avp-hidden-compatible
AC-FS(config-vpdn)#
```

【Verification】 Use the show running-config command to check whether the RFC2661 standard AVP Hidden parsing algorithm is supported.

【Prompt Information】

【Common Mistake】

【Platform Description】 -

18.18 l2tp tunnel force_ipsec

Configuring this command means that it is used together with IPSEC and is used in the case of external encryption, which means that packets must be encrypted to pass through the VPDN tunnel.

l2tp tunnel force_ipsec

Restore system default settings.

no l2tp tunnel force_ipsec

【Parameter Description】-

【Default Configuration】 By default, the system does not enable mandatory packet encryption.

【Command Mode】 VPDN-Group interface configuration mode

【Default Level】 14

【Usage Guide】Users can enable or disable the mandatory encryption function according to their needs. Any valid changes to the tunnel authentication function settings will cause the associated L2TP tunnel to be forcibly removed.

【Configuration Example】1: The system starts the mandatory encryption function.

```
AC-FS(config-vpdn)# l2tp tunnel force_ipsec
AC-FS(config-vpdn)#
```

【Verification】Use the show running-config command to check whether packets must be encrypted to pass through the VPDN tunnel

【Prompt Information】

【Common Mistake】

【Platform Description】 -

18.19 l2tp tunnel hello

Implements the Hello message sending interval for channel keepalives.

l2tp tunnel hello interval

Restore system default settings

no l2tp tunnel hello

【Parameter Description】

Parameter	Description
interval	The Hello message delivery interval, in seconds.

【Default Configuration】 By default, the system sets the Hello message sending interval to 60 seconds.

【Command Mode】 VPDN-Group interface configuration mode

【Default Level】 14

【Usage Guide】Users can set the Hello message sending interval according to their needs and network environment. Any valid changes to the channel Hello message sending interval setting will cause the corresponding L2TP tunnel to be forced and actively cleared

【Configuration Example】1: Set the sending interval of Hello message to 30 seconds.

```
AC-FS(config-vpdn)# l2tp tunnel hello 30
AC-FS(config-vpdn)#
```

【Verification】Using the show running-config command, you can view the sending interval of the Hello message of the channel Keepalive

【Prompt Information】

【Common Mistake】

【Platform Description】 -

18.20 l2tp tunnel password

Password for channel authentication.

l2tp tunnel password password-string

Clear the setting of the channel authentication password.

no l2tp tunnel password

【Parameter Description】

Parameter	Description
password-string	Channel Validation Password.

【Default Configuration】 By default, the system does not set the channel authentication password.

【Command Mode】 VPDN-Group interface configuration mode

【Default Level】 14

【Usage Guide】 If the user wants to perform tunnel authentication, both ends of the tunnel must enable the tunnel authentication function and use the same authentication password. Any valid changes to the settings of the tunnel authentication password will cause the corresponding L2TP tunnel to be forcibly removed.

【Configuration Example]】1: Set the channel authentication password to "share".

```
AC-FS(config-vpdn)# l2tp tunnel password share
AC-FS(config-vpdn)#
```

【Verification】Use the show running-config command to view the channel verification password

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

18.21 l2tp tunnel receive-window

Sets the size of the channel control message receiving window.

l2tp tunnel receive-window size

Restore system default settings.

no l2tp tunnel receive-window

【Parameter Description】

Parameter	Description
size	Channel control message accept window size.

【Default Configuration】 By default, the size of the channel control message receiving window is 4.

【Command Mode】 VPDN-Group interface configuration mode

【Default Level】 14

【Usage Guide】 Any valid change to the size of the channel control message receiving window size will cause the corresponding L2TP tunnel to be forcibly removed

【Configuration Example]】1: Set the size of the control message receiving window to 12.

```
AC-FS(config-vpdn)# l2tp tunnel receive-window 12
AC-FS(config-vpdn)#
```

【Verification】Use the show running-config command to view the size of the channel control message receiving window

【Prompt Information】

【Common Mistake】

【Platform Description】 -

18.22 l2tp tunnel retransmit

Set the L2TP channel control message retransmission Parameter.

l2tp tunnel retransmit { retries number | timeout { min | max } seconds }

Restore system default settings

no l2tp tunnel retransmit { retries | timeout { min | max } }

【Parameter Description】

Parameter	Description
number	Controls the number of message repasses.
seconds	Controls the message retransmission interval.

【Default Configuration】 By default, the maximum number of retransmissions of control messages is 5, the minimum interval for retransmission of control messages is 1 second, and the maximum interval is 8 seconds.

【Command Mode】 VPDN-Group interface configuration mode

【Default Level】 14

【 Usage Guide 】 Any effective modification to the channel control message retransmission Parameter setting will cause the corresponding L2TP tunnel to be forcibly removed.

【Configuration Example】1: Set the maximum number of retransmissions of control messages to 10.

```
AC-FS(config-vpdn)# l2tp tunnel retransmit retries 10
AC-FS(config-vpdn)#
```

【Verification】Use the show running-config command to view the L2TP channel control message retransmission Parameter

【Prompt Information】

【Common Mistake】

【Platform Description】 -

18.23 l2tp tunnel timeout

Sets the maximum session-less/control-connection interval allowed by L2TP.

l2tp tunnel timeout { no-session | setup } seconds

Restore system default settings

no l2tp tunnel timeout { no-session | setup }

【Parameter Description】

Parameter	Description
no-session	A channel established but not session.
setup	Control the unestablished connection (channel).
seconds	Time interval, measured in seconds.

【 Default Configuration 】 By default, the maximum time interval without a session allowed by the system is 600 seconds, and the maximum time for establishing a control connection (channel) allowed by the system is 300 seconds.

【Command Mode】 VPDN-Group interface configuration mode

【Default Level】 14

【Usage Guide】Any valid change to the setting of the maximum time interval for establishing a sessionless/control connection that is allowed on an existing channel will cause the associated L2TP tunnel to be forcibly removed.

【Configuration Example】1: Set the no-session interval allowed by the channel to 1200 seconds.

```
AC-FS(config-vpdn)# l2tp tunnel timeout no-session 1200
AC-FS(config-vpdn)#
```

【Verification】Use the show running-config command to view the maximum time interval without session/control connection allowed by L2TP

【Prompt Information】

【Common Mistake】

【Platform Description】 -

18.24 l2tp-class

Set the l2tp-class interface with the specified name. If there is no interface with the corresponding name, create an l2tp-class interface with the specified name.

l2tp-class l2tp-class-name

removes the l2tp-class interface of the specified name.

no l2tp-class l2tp-class-name

【Parameter Description】

Parameter	Description
l2tp-class-name	Name of the L2TP-Class interface

【Default Configuration】 By default, the system does not set any L2TP-Class interface.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】Users can configure and refer to L2TP-Class to realize the setting of working parameters of L2TP control connection

【Configuration Example]】1: The system creates an L2TP-Class interface named "l2x".

```
AC-FS(config)# l2tp-class l2x
AC-FS(config-l2tp-class)#
```

【Verification】Use the show running-config command to view the l2tp-class interface of the specified name

【Prompt Information】

【Common Mistake】

【Platform Description】 -

18.25 lcp renegotiation always

Ignore the errors of the L2TP control packets sent by the peer device that do not conform to the RFC specification, so that the negotiation can proceed normally.

lcp renegotiation always

Restore system default settings.

no lcp renegotiation always

【Parameter Description】-

【Default Configuration】 By default, the received L2TP control packets must strictly conform to the specification.

【Command Mode】 VPDN-Group interface configuration mode

【Default Level】 14

【Usage Guide】 It is used to ignore the errors of the L2TP control packets sent by the other device that do not conform to the RFC specification, so that the negotiation can proceed normally.

【Configuration Example】1: Set up tunnel re-authentication PPP LCP.

```
AC-FS(config-vpdn)# lcp renegotiation always
AC-FS(config-vpdn)#
```

【Verification】Use the show running-config command to check whether to ignore the errors of the L2TP control packets that do not conform to the RFC specification sent by the other device.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

18.26 local name

Set the hostname of the local side of the tunnel.

local name local-hostname-string

Restore system default settings.

no local name

【Parameter Description】

Parameter	Description
local-hostname-string	Local-end host name of the tunnel.

【Default Configuration】 By default, the system uses the name of the router as the string of the host name at the local end of the tunnel.

【Command Mode】 VPDN-Group interface configuration mode

【Default Level】 14

【Usage Guide】Users can set the local host name of the tunnel on the router to identify the tunnel. The valid settings or changes of this command will immediately cause the existing related tunnels to be actively forcibly removed.

【Configuration Example]】1: Set the local host name of the tunnel to "LNS".

```
AC-FS(config-vpdn)# local name LNS
AC-FS(config-vpdn)#
```

【Verification】Use the show running-config command to view the host name of the local end of the tunnel

【Prompt Information】

【Common Mistake】

【Platform Description】 -

18.27 password (L2TP)

Set the password for channel authentication.

password password-string

Restore system default settings

no password

【Parameter Description】

Parameter	Description
password-string	Password used for channel authentication

【Default Configuration】 By default, the system disables the channel authentication function and naturally does not set a password for channel authentication.

【Command Mode】 L2TP-Class interface configuration mode

【Default Level】 14

【Usage Guide】 If the user wants to perform tunnel authentication, both ends of the tunnel must enable the tunnel authentication function and use the same authentication password. Any valid changes to the settings of the tunnel authentication password will cause the corresponding L2TP tunnel to be forcibly removed.

【Configuration Example]】1: Set the channel authentication password to "share".

```
AC-FS(config-l2tp-class)# password share
AC-FS(config-l2tp-class)#
```

【Verification】Use the show running-config command to view the channel verification password

【Prompt Information】-

【Common Mistake】

【Platform Description】 -

18.28 pptp flow-control receive-window

Defines the maximum number of packets that the peer end of the pptp session is allowed to send before receiving the ack from the local end.

pptp flow-control receive-window packets

Restore system default settings

no pptp flow-control receive-window

【Parameter Description】

Parameter	Description
packets	The maximum number of packets that the peer end of the pptp session is allowed to send before receiving the ack from the local end. The value range is 1---64.

【Default Configuration】 The default value of PNS is 64, and the default value of PAC is 16.

【Command Mode】 vpdn-group configuration mode

【Default Level】 14

【Usage Guide】 This is a configuration command dedicated to the PPTP protocol, so the user must configure the protocol pptp or protocol any command before the system can display and configure this command.

According to the suggestion of PPTP protocol RFC2637, both sides of the session take half of the maximum receiving window of the other party received during the negotiation process as the initial sending window of the local end. When the sending window is full, the system

will stop the session from sending packets to the peer end and halve the sending window until it is 1, and resume message sending after receiving the ACK of the sent message from the peer end. When sending several packets of the current window size to the other party continuously without ACK timeout, the sending window size of the local end is increased by 1 until it is equal to the maximum receiving window value of the opposite end. The time interval for waiting for ACK timeout, calculated using a special algorithm according to the recommendations of RFC2637. You must configure protocol pptp or protocol any before this command is displayed.

【Configuration Example]】 1: Configure the maximum receive window value of the pptp session at the local end to 32.

```
AC-FS(config-vpdn)# accept-dialin AC-
FS(config-vpdn-acc-in)# protocol pptp AC-
FS(config-vpdn-acc-in)# exit
AC-FS(config-vpdn)# pptp flow-control receive-window 32
AC-FS(config-vpdn)#
```

【Verification】 Use the show running-config command to view the maximum number of packets allowed to be sent

【Prompt Information】

【Common Mistake】

【Platform Description】 -

18.29 pptp flow-control static-rtt

Defines the static reference timeout for a pptp session to wait for an ACK response after sending a single data packet.

pptp flow-control static-rtt timeout-interval

Restore system default settings

no pptp flow-control static-rtt

【Parameter Description】

Parameter	Description
timeout-interval	The static reference timeout for the Ppt p session waiting for the message ACK response after sending a single data message time, in milliseconds.The value range is 100- - -5000

【Default Configuration】 The default value is 1500 milliseconds.

【Command Mode】 vpdn-group configuration mode

【Default Level】 14

【Usage Guide】 This is a configuration command dedicated to the PPTP protocol, so the user must configure the protocol pptp or protocol any command before the system can display and configure this command.

According to the recommendation of PPTP protocol RFC2637, the time interval (ATO, Acknowledgment Time-Outs) that PPTP waits for ACK timeout after sending a data packet is calculated using a special algorithm, which uses the dynamically calculated RTT (Round-Trip Time) time. The static-rtt time configured by this command is used as the reference initial value for RTT calculation

【Configuration Example]】1: Configure the maximum receive window value of the pptp session at the local end to 32.

```
AC-FS(config-vpdn)# accept-dialin AC-
FS(config-vpdn-acc-in)# protocol pptp
AC-FS(config-vpdn-acc-in)# exit
```

```
AC-FS(config-vpdn)# pptp flow-control static-rtt 32
AC-FS(config-vpdn)#
```

【Verification】Using the show running-config command, you can view the static reference timeout time for the pptp session to wait for the ACK response after sending a single data packet.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

18.30 pptp tunnel echo

Configure the interval at which the pptp tunnel actively sends the echo request.

pptp tunnel echo echo-packet-interval

Restore system default settings.

no pptp tunnel echo

【Parameter Description】

Parameter	Description
echo-packet-interval	Ppt p tunnel echo request message sending interval, in seconds.The value range is 0---1000.

【Default Configuration】 The default interval is 60 seconds.

【Command Mode】 vpdn-group configuration mode

【Default Level】 14

【Usage Guide】 This is a configuration command dedicated to the PPTP protocol, so the user must configure the protocol pptp or protocol any command before the system can display and configure this command. When echo-packet-interval is set to 0, echo packets will not be sent actively.

When the echo-packet-interval is not 0, the PPTP tunnel does not receive any legal protocol or data packet from the peer end within the continuous echo-packet-interval seconds, then it actively sends an echo request to detect the status of the tunnel, and Start timing to wait for the echo reply from the peer. The initial waiting time for a response is 1 second. If the first response times out, the second echo request will be sent immediately, and the waiting time for a response will be doubled on the basis of the previous one, and so on. If it fails to receive the echo reply from the peer for 5 consecutive times, it is considered that the tunnel communication is abnormal, and the tunnel and the session it contains will be closed. You must configure protocol pptp or protocol any before this command is displayed.

【Configuration Example]】1: Configure pptp echo request to be 30 seconds.

```
AC-FS(config-vpdn)# accept-dialin AC-
FS(config-vpdn-acc-in)# protocol pptp AC-
FS(config-vpdn-acc-in)# exit AC-FS(config-
vpdn)# pptp tunnel echo 30
AC-FS(config-vpdn)#
```

【Verification】Using the show running-config command, you can view the interval between the pptp tunnel actively sending the echo request

【Prompt Information】

【Common Mistake】

【Platform Description】 -

18.31 protocol

Set up the tunnel to use the tunneling protocol.

protocol { any | l2tp | pptp }

Restore system default settings.

no protocol

【Parameter Description】

Parameter	Description
any	Match all of the tunnel protocols available.
l2tp	Match the tunnel protocol L2TP.
Pptp	Match the tunnel protocol PPTP.

【Default Configuration】 By default, the system does not specify the configured tunnel protocol for the tunnel.

【Command Mode】 VPDN-Group tunnel working mode interface configuration mode

【Default Level】 14

【Usage Guide】 The user must specify the tunnel protocol used by the tunnel. Any valid settings or changes to the tunnel protocol will cause all existing related tunnels to be removed actively. The accept-dialin command must be configured first before this command is displayed.

【Configuration Example】1: Set the tunnel protocol to L2TP.

```
AC-FS(config-vpdn)# accept-dialin
AC-FS(config-vpdn-acc-in)# protocol l2tp
AC-FS(config-vpdn-acc-in)#
```

【Verification】Use the show running-config command to view the tunnel protocol used by the tunnel

【Prompt Information】

【Common Mistake】

【Platform Description】 -

18.32 protocol (L2TP)

Set the L2TP control connection parameter.

protocol l2tpv2 [l2tp-class-name]

Restore system default settings.

no protocol

【Parameter Description】

Parameter	Description
l2tpv2	The L2TP was used as a tunnel protocol.
l2tp-class-name	Reenced L2TP-Class interface name.

【Default Configuration】 By default, the system uses L2TPv2 as the L2TP tunnel protocol by default.

【Command Mode】 Pseudowire-Class interface configuration mode

【Default Level】 14

【Usage Guide】 Any valid changes to the control connection parameter settings will cause the corresponding L2TP tunnel to be forcibly removed.

【Configuration Example]】1: Set the tunnel protocol to l2tpv2 and apply L2TP-Class l2x to set the control connection Parameter.

```
AC-FS(config-pw-class)# protocol l2tpv2 l2x
AC-FS(config-pw-class)#
```

【Verification】Use the show running-config command to view the L2TP control connection Parameter

【Prompt Information】

【Common Mistake】

【Platform Description】 -

18.33 pseudowire

Set pseudowire rules.

Pseudowire peer-ip-address vcid { encapsulation l2tpv2 [pw-class pw-class-name] | pw-class pw-class-name }

Restore system default settings

no pseudowire

Configure pseudowire with hostname Parameter

pseudowire hostname peer-hostname vcid { encapsulation l2tpv2 [pw-class pw-class-name] | pw-class pw-class-name }

Restore system default settings

no pseudowire

【Parameter Description】

Parameter	Description
peer-ip-address	The remote L2TP Server (LNS) address.
peer-hostname	Remote L2TP Serve (r LNS) The hostname registered on the DNS corresponding to its address.
vcid	pseudowire global markup volume.
l2tpv2	Use the l2tpv2 (RFC 2661) as a tunnel protocol.
pw-class-name	Name of the referenced pseudowire-class unit.

【Default Configuration】 By default, the system does not set any pseudowire rules.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 pseudowire rules can only be configured on virtual-ppp interfaces. Any valid changes to the pseudowire rules on the virtual-ppp interface will cause the corresponding L2TP session to be forcibly torn down.

【Configuration Example】 1 : Set pseudowire rules on virtual-ppp interface, which set LNS address to 192.168.12.213 and refer to

pseudowire-class interface "pw"

```
AC-FS(config)# interface virtual-ppp 1
AC-FS(config-if)# pseudowire 192.168.12.213 33 pw-class pw
AC-FS(config-if)#
```

2: hostname configuration example:

Open the DNS service, configure the DNS server address, configure the route to the server.

```
ip domain-lookup
l2tp-class 1
pseudowire-class 1
 encapsulation l2tpv2
ip name-server 192.168.5.119
ip name-server 61.154.22.41
interface FastEthernet 0/0
 ip ref
 ip address 192.168.52.90 255.255.255.0
 duplex auto
 speed auto
interface Virtual-ppp 1
 pseudowire hostname mm.hxs.meibu.com 1 encapsulation l2tpv2
 ppp pap sent-username user1 password  11
 ip address negotiate
ip route 0.0.0.0 0.0.0.0 192.168.52.1
```

【Verification】 Use the show running-config command to view the pseudowire rules

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

18.34 pseudowire-class

Sets the pseudowire-class interface with the specified name, or creates a pseudowire-class interface with the specified name if there is no pseudowire-class interface with the specified name.

pseudowire-class pseudowire-class-name

removes the pseudowire-class interface of the specified name.

no pseudowire-class pseudowire-class-name

【Parameter Description】

Parameter	Description
pseudowire-class-name	pseudowire-class Interface name.

【Default Configuration】 By default, no pseudowire-class interface is set on the system.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Users can configure and refer to the pseudowire-class interface to set the L2TP tunnel working Parameter

【Configuration Example]】 1: Create a pseudowire-class interface named "pw".

```
AC-FS(config)# pseudowire-class pw
AC-FS(config-pw-class)#
```

【Verification】 Use the show running-config command to view the pseudowire-class interface of the specified name。

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

18.35receive-window

Sets the size of the tunnel control message receiving window.

receive-window size

Restore system default settings.

no receive-window

【Parameter Description】

Parameter	Description
size	Controls the message acceptance window dimensions.

【Default Configuration】 By default, the size of the control message receiving window is 8.

【Command Mode】 L2TP-Class interface configuration mode

【Default Level】 14

【Usage Guide】Any valid change to the size of the tunnel control message receiving window will cause the corresponding L2TP tunnel to be forcibly removed.

【Configuration Example]】1: Set the size of the control message receiving window to 12.

```
AC-FS(config-l2tp-class)# receive-window 12
AC-FS(config-l2tp-class)#
```

【Verification】Use the show running-config command to view the size of the tunnel control message receiving window

【Prompt Information】

【Common Mistake】

【Platform Description】 -

18.36 retransmit

Set the control message retransmission Parameter.

retransmit {initial {retries initial-retries | timeout {max | min} initial-timeout} | retries retries | timeout {max | min} timeout}

Restore system default settings.

no retransmit { initial {retries | timeout {max | min} }| retries | timeout {max | min} }

【Parameter Description】

Parameter	Description
initial-retries	SCCRQ number of repasses with a value range of 1-1000.
initial-timeout	For the SCCRQ retransmission time interval, the value range is 1-8.
retries	Others control the number of messages that range from 5-1000.
timeout	Other control message retransmission time interval, take the value range of 1-8.

【Default Configuration】 By default, the number of SCCRQ retransmissions is 2, and the number of other control messages is 5. The minimum interval for retransmission of control messages is 1 second, and the maximum interval for retransmission of control messages is 8 seconds.

【Command Mode】 L2TP-Class interface configuration mode

【Default Level】 14

【Usage Guide】 Any effective change to the control message retransmission Parameter setting will cause the corresponding L2TP tunnel to be forcibly removed.

【Configuration Example】1: Set the SCCRQ retransmission times to 3.

```
AC-FS(config-l2tp-class)# retransmit initial retries 3
AC-FS(config-l2tp-class)#
```

【Verification】Use the show running-config command to view the control message retransmission Parameter

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

18.37 show l2tp-class

Display the configuration information of the specified l2tp-class interface on the current system

show l2tp-class [l2tp-class-name]

【Parameter Description】

Parameter	Description
l2tp-class-name	Specify the name of the l2tp-class

【Default Configuration】-

【Command Mode】 Normal user mode, privileged user mode

【Default Level】 14

【Usage Guide】 Users can use this command to view the detailed configuration information of all l2tp-class interfaces or specified l2tp-class interfaces in the current system configuration.

【Configuration Example]】1: Display the detailed configuration information of all l2tp-class interfaces on the current system.

```
AC-FS# show l2tp-class
```

```
L2TP Class class-default:
  hidden disable, authentication disable
  hello interval 60 second(s)
  hostname Router, password Router
  timeout setup 120 seconds
  receive-window 8, no cookie space
  retransmit retries 5, retransmit initial retries 2
  retransmit timeout max 8 second(s), retransmit timeout min 1 second(s)
  retransmit initial timeout max 8 second(s)
  retransmit initial timeout min 1 second(s)

L2TP Class l2x:
  hidden disable, authentication disable
  hello interval 60 second(s)
  hostname Router, password Router
  timeout setup 120 seconds
  receive-window 8, no cookie space
  retransmit retries 5, retransmit initial retries 2
  retransmit timeout max 8 second(s), retransmit timeout min 1 second(s)
  retransmit initial timeout max 8 second(s)
  retransmit initial timeout min 1 second(s)
AC-FS#
```

2: Display the detailed configuration information of the l2tp-class interface of the specified name

```
AC-FS# show l2tp-class l2x
L2TP Class l2x:
  hidden disable, authentication disable
  hello interval 60 second(s)
  hostname Router, password Router
  timeout setup 120 seconds
  receive-window 8, no cookie space
  retransmit retries 5, retransmit initial retries 2
```

Field Description:

Field	Instruction
hidden	Is the avp hidden and the disable not hidden.
authentication	Whether tunnel certification is supported, and disable does not support tunnel certification.
hello interval	The interval between sending a hello message.
timeout setup	Set the maximum time allowed for building control connections.
receive-window	The Tunnel control message accepts the window size.
retransmit retries	Number of other control messages (except SCCRQ).
retransmit initial retries	Number of SCCRQ messages.
retransmit timeout max	Maximum value of the retransmission interval for other control messages (except SCCRQ).
retransmit timeout min	Minimum value of the retransmission interval for other control messages (except SCCRQ).
retransmit initial timeout max	Maximum time interval of SCCRQ message retransmission.
retransmit initial timeout min	Minimum value of the SCCRQ message retransmission time interval.
reference count	The number of pseudowire-class interfaces associated with the l2tp-class interface.

【Prompt Information】 -

【Platform Description】 -

18.38show pseudowire-class

Displays configuration information for the specified pseudowire-class interface on the current system

show pseudowire-class [pseudowire-class-name]

【Parameter Description】

Parameter	Description
l2tp-class-name	Specify the pseudowire-class interface name.

【Default Configuration】 -

【Command Mode】 Normal user mode, privileged user mode

【Default Level】 14

【**Usage Guide**】Users can use this command to view the detailed configuration information of all pseudowire-class interfaces or specified pseudowire-class interfaces in the current system configuration.

【**Configuration Example**】1: Display the detailed configuration information of all pseudowire-class interfaces on the current system.

```
AC-FS# show pseudowire-class

Pseudowire Class pw:
  encapsulation l2tpv2, protocol l2tpv2 on l2tp-class l2x
  ip dfbit set disable, ip pmtu disable, ip ttl 255
  ip tos reflect disable, ip tos value 0
  reference count: 1000

Pseudowire Class pw1:
  encapsulation l2tpv2
  ip dfbit set disable, ip pmtu disable, ip ttl 255
  ip tos reflect disable, ip tos value 0
  reference count: 0

Pseudowire Class pw2:
  encapsulation l2tpv2, protocol l2tpv2 on l2tp-class l2x
  ip dfbit set disable, ip pmtu disable, ip ttl 255
  ip tos reflect disable, ip tos value 0
  reference count: 0 AC-
FS#
```

2: Display detailed configuration information of the pseudowire-class interface of the specified name

```
AC-FS# show pseudowire-class pw

Pseudowire Class pw:
  encapsulation l2tpv2, protocol l2tpv2 on l2tp-class l2x
  ip dfbit set disable, ip pmtu disable, ip ttl 255
```

Field Description:

Field	Instruction
encapsulation	The protocol for encapsulation.
protocol	The protocol used.
l2tp-class	Associated l2tp-class interface.
ip dfbit	Whether the tunnel data allows for fragmentation.
ip ttl	The TTL domain of the IP header loading the tunnel data.
ip tos	The IP header TOS (Type of Service) domain of the load tunnel.
reference count	The number of virtual-ppp interfaces associated with the pseudowire-class interface.

【Prompt Information】-

【Platform Description】 -

18.39 show vpdn

Displays the specified VPDN tunnel information on the current system.

show vpdn [session | tunnel [{ l2tp | pptp } locid]]

【Parameter Description】

Parameter	Description
session	Show all of the sessions.
tunnel	Displays all channels.
l2tp locid	Displays the details of the L2TP tunnel for the specified id.The value range is 1-65535.
pptp locid	Displays the details of the PPTP tunnel for the specified id.The value range is 0-65535.

【Default Configuration】-

【Command Mode】 Normal user mode, privileged user mode

【Default Level】 14

【Usage Guide】The user can use this command to inspect the VPDN tunnel information on the current system in real time. If Parameter is

not specified, all VPDN channels and sessions on the current system will be displayed.

Note: Since the length of the user name is arbitrary, in order to align the format, it is stipulated during show that only the length of the first 12 bytes of the user name will be displayed.

If you want to display the full username, you can use show vpdn tunnel l2tp locid , show vpdn tunnel pptp locid to view.

【Configuration Example]】1: Check all VPDN tunnel information on the current system.

```
AC-FS# show vpdn
L2TP Tunnel and Session Information Total tunnels 1 sessions 1
LocID RemID Remote Name State  Remote Address  Port  Sessions L2TP Class/
VPDN Group
4     77    BLIZZARD      est.....192.168.12.213  1701  1        1
LocID       RemID       TunID       Username, Intf/      State  Last Chg
                                    Vcid, Circuit
1           1           4           ms,Vi1               est    00:33:58
%No active PPTP tunnels AC-
FS#
```

Displays information about all VPDN tunnels on the current system.

```
AC-FS# show vpdn tunnel
L2TP Tunnel Information Total tunnels 1
LocID RemID Remote Name State  Remote Address  Port  Sessions L2TP Class/
VPDN Group
4     77    BLIZZARD      est.....192.168.12.213  1701  1        1
%No active PPTP tunnels AC-
FS#
```

Displays information about all VPDN sessions on the current system

```
AC-FS# show vpdn session
L2TP Session Information Total sessions 1
LocID       RemID       TunID       Username, Intf/      State  Last Chg
                                    Vcid, Circuit
1           1           4           ms,Vi1               est    00:37:03
%No active PPTP tunnels AC-
FS#
```

2: Display the specified PPTP or L2TP tunnel details.

Display the detailed information of the L2TP tunnel whose specified tunnel id is the specified value:

```
AC-FS# show vpdn tunnel l2tp 4
L2TP tunnel locid 4 is up,remote id is 77, 1 active sessions
  Tunnel state is est
  Tunnel transport is UDP
  Remote tunnel name is BLIZZARD
    Internet Address 192.168.12.213, port 1701
  Local tunnel name is LNStest
    Internet Address 192.168.12.212, port 1701
  VPDN group for tunnel is 1
  Tunnel domain unknown
  ip mtu adjust disabled
  Control Ns 2, Nr 4
```

Display the detailed information of the PPTP tunnel whose specified tunnel id is the specified value:

```
AC-FS#show vpdn tunnel
%No active L2TP tunnels
PPTP Tunnel Information Total tunnels 1
LocID Remote Name     State       Remote Address  Port  Sessions
2                    estbed.............192.168.45.160  3077 1
AC-FS#
AC-FS#show vpdn tunnel pptp 2
PPTP tunnel id 2 is up, remote id is 0, 1 active session
  Tunnel state is estbed
  Remote tunnel name is
    Internet Address 192.168.45.160, port 3077
  Local tunnel name is
    Internet Address 192.168.45.161
```

Field Description:

Field	Instruction
L2TP Tunnel	L2TP channel
Session Information	Session information
LocID	this locality,ID

RemID	far-end,ID
TunID	channel,ID
Username, Intf:	User name and interface
State	state
Last Chg	Finally change the time
Remote Address	The paired-end address
Port	Port

【Prompt Information】-

【Platform Description】 -

18.40 show vpdn log

Displays the user online and offline information saved in the current log file

show vpdn log [user username]

【Parameter Description】

Parameter	Description
username	The user name specified.

【Default Configuration】-

【Command Mode】 Normal user mode, privileged user mode

【Default Level】 14

【Usage Guide】 The user can use this command to view the online and offline information of all or specified users in the current log file.

【Configuration Example]】1: Display all user log on and off line information in the current log file

```
AC-FS# show vpdn log

Username                IP              State   Online time          Offline time
user-1                  100.1.1.2       out     2014-11-16-14:09:04  2014-11-16-14:29:26
```

```
user-2          100.1.2.2    out    2014-11-16-15:09:05    2014-11-16-16:09:27

user-3          100.1.3.2    out    2014-11-16-17:09:04    2014-11-16-18:09:26

user-4          100.1.4.2    in     2014-11-16-18:09:05

AC-FS#
```

2: Display the online and offline information of the specified user in the current log file.

```
AC-FS# show vpdn log user user-1
```

```
Username                        IP          State  Online time          Offline time
user-1                          100.1.1.2   out    2014-11-16-14:09:04  2014-11-16-14:29:26
AC-FS#
AC-FS#show vpdn log user AC-FS
%No vpdn logs for username: AC-FS.  AC-FS#
```

【Prompt Information】-

【Platform Description】 First supported item 11_1_PJ5

18.41 source-ip

Set the tunnel corresponding to the current VPDN-Group to use the local (source) address.

source-ip A.B.C.D

Restore system default settings.

no source-ip

【Parameter Description】

Parameter	Description
A.B.C.D	The current VPDN-Group corresponds to the local (source) address used in the

	tunnel.

【Default Configuration】 By default, the system does not restrict the local (source) address used by the VPDN-Group to establish a tunnel.

【Command Mode】 VPDN-Group interface configuration mode

【Default Level】 14

【Usage Guide】 If the local (source) address used by the global VPDN function has been set, the local (source) address used by the VPDN-Group when establishing the tunnel must be the same. The effective settings or changes of this command will immediately cause the existing related tunnels to be actively forcibly removed.

【Configuration Example]】 1: Set the source address used by the current VPDN-Group to 202.101.92.73.

```
AC-FS(config-vpdn)# source-ip 202.101.92.73
AC-FS(config-vpdn)#
```

【Verification】 Use the show running-config command to view the local (source) address used by the tunnel corresponding to the current VPDN-Group.

【Prompt Information】

【Common Mistake】

【Platform Description】 -

18.42 terminate-from

Specifies the host name of the peer end of the tunnel.

terminate-from hostname remote-hostname-string

Restore system default settings.

no terminate-from

【Parameter Description】

Parameter	Description
remote-hostname-string	Tunnel end-to-end host name.

【Default Configuration】 By default, the system does not set the peer host name of the tunnel.

【Command Mode】 VPDN-Group interface configuration mode

【Default Level】 14

【Usage Guide】 The user can use this command to restrict the remote access user host name. If the tunnel peer host name is not set, the VPDN-Group will not restrict the remote access user host name. Any valid change to the remote host name of the tunnel will cause all existing tunnels corresponding to the VPDN-Group to be forcibly removed.

【Configuration Example]】1: Set the host name of the peer end of the tunnel to "LAC".

```
AC-FS(config-vpdn)# terminate-from hostname LAC
AC-FS(config-vpdn)#
```

【Verification】Use the show running-config command to view the host name of the peer end of the tunnel

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

18.43timeout setup

Sets the maximum time the system allows to establish a control connection.

timeout setup seconds

Restore system default settings

no timeout setup

【Parameter Description】

Parameter	Description

seconds	The maximum time allowed by the system to establish a control connection takes in seconds.The value range is 60-6000.

【Default Configuration】 By default, the maximum time allowed by the system to establish a control connection is 120 seconds.

【Command Mode】 L2TP-Class interface configuration mode

【Default Level】 14

【Usage Guide】 Any valid modification to the maximum time allowed to establish a control connection by the system will cause the related L2TP tunnel to be forcibly cleared.

【Configuration Example]】1: Set the maximum time allowed by the system to establish a control connection to 240 seconds.

```
AC-FS(config-l2tp-class)# timeout setup 240
AC-FS(config-l2tp-class)#
```

【 Verification 】Use the show running-config command to view the maximum time allowed by the system to establish a control connection

【Prompt Information】

【Common Mistake】

【Platform Description】 -

18.44 virtual-template

Set the virtual template interface bound to the current VPDN-Group.

virtual-template number

Restore system default settings.

no virtual-template

【Parameter Description】

Parameter	Description
number	The virtual template interface serial number, and the value range is 1-1200.

【Default Configuration】 By default, the system does not bind any virtual template interface to the VPDN-Group.

【Command Mode】 VPDN-Group tunnel working mode interface configuration mode

【Default Level】 14

【Usage Guide】 Users can use this command to bind the virtual template interface used by VPDN-Group to determine the network interface parameters of the load session. If you want the VPDN-Group to provide it, you must bind the virtual template interface. Any valid change to the virtual template interface bound to the VPDN-Group will cause the existing tunnel corresponding to the VPDN-Group to be forcibly removed.

It can only be configured after the protocol configuration is configured, otherwise the command will not be visible.

【Configuration Example]】1: Bind virtual template interface 1 to the VPDN-Group where it belongs.

```
AC-FS(config)# AC-FS(config)#vpdn-
group 1 AC-FS(config-vpdn)#accept-
dialin
AC-FS(config-vpdn-acc-in)#protocol any AC-
FS(config-vpdn-acc-in)#virtual-template 1
AC-FS(config-vpdn-acc-in)#
```

【Verification】Use the show running-config command to view the virtual template interface bound to the current VPDN-Group.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

18.45vpdn congestion_avoidanc

Enable VPDN congestion control.

vpdn congestion_avoidanc

Disable VPDNVPDN congestion control.

no vpdn congestion_avoidanc

【Parameter Description】-

【Default Configuration】 By default, the system disables the VPDN congestion control function.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】Users can decide whether to enable congestion control according to the current network environment.

【Configuration Example]】1: The system enables the VPDN congestion control function.

```
AC-FS#config
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)# vpdn congestion_avoidanc
AC-FS(config)#
```

【Verification】Use the show running-config command to check whether the VPDN function is enabled

【Prompt Information】-

【Prompt Information】-

【Platform Description】 -

18.46 vpdn enable

Enable VPDN functionality.

vpdn enable

Disable VPDN functionality.

no vpdn enable

【Parameter Description】-

【Default Configuration】 By default, the system disables the VPDN function.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】Except that the L2TP tunnel initiated by the client (Client-Initiated Tunnel) does not require the system to enable the VPDN function, whether RGOS provides the LAC or LNS function, and whether it uses the PPTP or L2TP protocol, the system requires the system to enable the VPDN function. The valid settings or changes of this command will immediately cause the existing related tunnels to be actively forcibly removed.

【Configuration Example】1: The system enables the VPDN function.

```
AC-FS#config
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)# vpdn enable
AC-FS(config)#
```

【Verification】Use the show running-config command to check whether the VPDN function is enabled.

【Prompt Information】

【Common Mistake】

【Platform Description】 -

18.47 vpdn ignore_source

Enable the VPDN source-to-site ignore function. After this command is enabled, the data packets sent by the other party will not be checked for source address matching.

vpdn ignore_source

Strictly check the source address of the peer packet.

no vpdn ignore_source

【Parameter Description】-

【Default Configuration】 By default, the system checks the source address matching of tunnel packets.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】This command enables the VPDN source-to-site ignore function. After this command is enabled, the data packets sent by the other party will not be checked for source address matching. Only useful for fast-forwarding data.

【Configuration Example】1: The system enables the function of ignoring the VPDN source address.

```
AC-FS(config)# vpdn ignore_source
AC-FS(config)#
```

【Verification】Use the show running-config command to check whether the VPDN source-to-site ignore function is enabled.

【Prompt Information】

【Common Mistake】

【Platform Description】

18.48 vpdn limit_rate

Set the number of tunnels allowed to be established per second for VPDN provided by the current system, and limit the establishment speed of VPDN.

vpdn limit_rate rate_num

Turn off the connection rate limit for VPDN.

no vpdn limit_rate

【Parameter Description】

Parameter	Description
rate_num	5-100, the number of VPDN tunnels allowed to be established per second by the system is a minimum of 5 and a maximum of 100.

【Default Configuration】 10.x does not limit the speed of the VPDN tunnel establishment process by default. The revision of 11.x is to

limit the speed of the VPDN tunnel establishment process by default. The default value is 15 routes per second.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 When there are too many VPDN dial-in at the same time, which affects the overall performance of the system, you can use this command to limit the number of dial-in.

【Configuration Example]】1: Set the currently accepted number of negotiated tunnels per second to 50.

```
AC-FS(config)# vpdn limit_rate 50
AC-FS(config)#
```

【Verification】Using the show running-config command, you can view the number of tunnels that the VPDN is allowed to establish per second.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

18.49 vpdn session-limit

Sets the maximum number of sessions allowed when the current system provides the VPDN function.

vpdn session-limit sessions

Restore system default settings.

no vpdn session-limit

【Parameter Description】

Parameter	Description
sessions	The maximum number of sessions allowed when the system provides VPDN functionality, in a range of 1-300.

【Default Configuration】 By default, this value is set to the maximum number of sessions that the system can provide, of which 300 for

36 series.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 When there are too many VPDN dial-ins at the same time, which affects the overall performance of the system, you can use this command to limit the dial-in number. The vpdn enable command must be enabled first.

【Configuration Example】1: Set the maximum number of sessions currently accepted to 100.

```
AC-FS(config)# vpdn session-limit 100
AC-FS(config)#
```

【Verification】Use the show running-config command to view the maximum number of sessions allowed when the current system provides the VPDN function

【Prompt Information】

【Common Mistake】

【Platform Description】

18.50vpdn source-ip

Set the local (source) address used by the current system to provide the VPDN function.

vpdn source-ip A.B.C.D

Restore system default settings.

no vpdn source-ip A.B.C.D

【Parameter Description】

Parameter	Description
A.B.C.D	The local address used when the system provides the VPDN functionality.

【Default Configuration】 By default, the system does not set the local (source) address used for providing the VPDN function.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 If the system provides LNS(L2TP) or HGW(PPTP) function, you can use this command to limit the destination address of all currently accepted tunnel connection requests to the set address. The valid settings or changes of this command will immediately cause the existing related tunnels to be actively forcibly removed. The vpdn enable command must be enabled first.

【Configuration Example]】1: Set the destination address of all currently accepted tunnel connection requests to 192.168.12.223.

```
AC-FS(config)# vpdn source-ip 192.168.12.223
AC-FS(config)#
```

【Verification】Use the show running-config command to view the local (source) address used by the current system to provide the VPDN function.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

18.51vpdn-group

Set the VPDN-Group interface with the specified name. If there is no corresponding VPDN-Group interface, create a VPDN-Group interface with the specified name as the name.

vpdn-group vpdn-group-name

Delete the VPDN-Group interface of the specified name.

no vpdn-group vpdn-group-name

【Parameter Description】

Parameter	Description
vpdn-group-name	Name of the vpdn-group interface.

【Default Configuration】 By default, the system does not set any vpdn-group interface.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 If the user wants the router to act as LNS or HGW, he must create and set the VPDN-Group interface. Users can use this command to manage the VPDN-Group interface. Deletion of the VPDN-Group interface will directly cause the corresponding existing tunnel to be actively forcibly removed. The vpdn enable command must be enabled first.

【Configuration Example]】1: Create a vpdn-group interface named "1".

```
AC-FS(config)# AC-
FS(config)#vpdn enable AC-
FS(config)#vpdn-group 1
AC-FS(config-vpdn)#
```

【Verification】Use the show running-config command to view the VPDN-Group interface with the specified name.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

19 AD Configuration Commands

19.1 advertising enable

Start ad serving globally. Compatible with the original advertising webauth-free-user command.

advertising enable

Disable mobile ad serving globally.

no advertising enable

【Parameter Description】-

【Default Configuration】 There is no setting by default.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】 To successfully apply the advertisement service, you must configure the network segment range for advertisement push and the page address of the advertisement popup box.

【Configuration Example】1: Enable advertisement.

```
AC-FS(config)# advertising enable
```

【Verification】Use show advertising to view the configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

19.2 advertising url

Set the page address of the ad popup.

advertising url url-string

Delete the page address of the ad popup.

no advertising url

【Parameter Description】

Parameter	Description
url-string	The page address should start with "http://" or "https://", otherwise it will prompt that the configuration is unsuccessful, and the maximum length is 255 characters.

【Default Configuration】 There is no setting by default.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure url.

```
AC-FS(config)# advertising url http://www.baidu.com/
```

【Verification】Use show advertising to view the configuration

【Prompt Information】 1: Illegal url format.

```
%Warning: Illegal URL, ignored. URL can not point to a file, URL must point to a HTML page.
```

【Common Mistake】-

【Platform Description】 -

19.3 advertising suppress

Enable periodic interception.

advertising suppress

Turn off periodic interception.

no advertising suppress

【Parameter Description】-

【Default Configuration】 It is not enabled by default.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】 After the periodic interception is enabled, the default periodic interval is 30 minutes.

【Configuration Example]】1: Enable periodic interception.

```
AC-FS(config)# advertising suppress
```

【Verification】Use show advertising to view the configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

19.4 advertising min-interval

Set the interval for periodic interception.

advertising min-interval interval-value

Remove the interval for periodic interception.

no advertising min-interval

【Parameter Description】

Parameter	Description
interval-value	Interval values were <30–1440> in points, with a default of 30 min.

【Default Configuration】 After periodic interception is enabled, the default interception interval is 30 minutes.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】 12. Periodic interception is not enabled, the default is 0.

13. Enable periodic interception, the default is 30.

14. After the periodic interception is enabled, there will be an error in deleting the configuration.

【Configuration Example】1: Set the interval for periodic interception.

```
AC-FS(config)# advertising min-interval 30
```

【Verification】Use show advertising to view the configuration.

【Prompt Information】 1: After the periodic interception is enabled, it is not allowed to delete the time interval configuration.

```
%Warning: Should set min-interval to default value: 30mins, due to advertising suppress.
```

【Common Mistake】-

【Platform Description】 -

19.5 advertising free-user

Set the network segment range for ad push. Compatible with the original webauth-free-user address < ip-address > mask < ip-mask> command.

advertising free-user ip < ip-address > mask < ip-mask >

Delete a network segment range.

no advertising free-user ip < ip-address > mask < ip-mask >

【Parameter Description】

Parameter	Description
ip-address	The ip address, point in decimal format.
ip-mask	Subnet mask, dot-point decimal format.

【Default Configuration】 The default is not configured.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】 Only supports the configuration of up to 50 network segments.

【Configuration Example】1: Set a certain network segment.

```
AC-FS(config)# advertising free-user ip 192.168.198.1 mask 255.255.255.0
```

2: Configure the entire network segment. Compatible with the original advertising all-user without-webauth command

```
AC-FS(config)# advertising free-user ip 0.0.0.0 mask 255.255.255.255
```

【Verification】-

【Prompt Information】 1: Configure the 51st network segment.

```
%Error: Has reached the 50 rules limit.
```

【Common Mistake】-

【Platform Description】 -

19.6 show advertising

Basic configuration for displaying ads.

show advertising

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Used to view the basic Parameter configuration of advertisements.

【Configuration Example】1: Basic configuration for displaying advertisements.

```
AC-FS#show advertising
advertising enable:       On
advertising url:          http://www.baidu.com/
advertising suppress:     On
advertising  popup-page:  On
advertising min-interval: 30
advertising free-user:
  192.168.198.0   255.255.255.0
  1.1.1.1         255.255.0.0
```

Field Description:

Field	Instruction
advertising popup-page	Display only when turned on.
advertising free-user	Display only when there is a network segment configuration.

【Prompt Information】-

【Platform Description】 -

19.7 show advertising free-user

Displays the range of network segments to which the advertiser belongs. Compatible with the original show webauth-free-user command.

show advertising free-user

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 It is used to check the network segment range to which the advertiser belongs.

【Configuration Example】1: Display the network segment range to which the advertiser belongs.

```
AC-FS#show advertising free-user

free-user configuration:

  Address          Mask

  ______________  ______________

  192.168.198.0    255.255.255.0

  1.1.1.1          255.255.0.0

  2.2.2.2          255.0.0.0
```

Field Description

Field	Instruction
Address	IP address.
Mask	IP address mask.

【Prompt Information】-

【Platform Description】 -

19.8 show advertising user

Displays a linked list of ad user timeouts (push intervals). Compatible with the original show advertising tmo command.

show advertising user

【Parameter Description】

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Used to view the list of advertisement user timeout (push interval)

【Configuration Example]】1: Display a list of advertisement user timeouts (push interval).

```
AC-FS(config)#show adv user
Current online advertising user num: 1
Address         Online  Time Limit     Time used      Name
--------------- ------- -------------- -------------- --------

192.168.198.34  On      0d 00:30:00    0d 00:08:50    AD_USER
```

Field Description:

Field	Instruction
Address	IP address.
Online	Online status.
Time Limit	Push interval.
Time used	Online time.
Name	Default user name: AD_USER.

【Prompt Information】-

【Platform Description】 -

Chapter 10 System Configuration

This volume introduces the contents of the system configuration command manual, including the following chapters:

1. Command Line Interface
2. Basic configuration management
3. LINE
4. RMON
5. File System
6. SNMP
7. HTTP
8. System log
9. RLOG
10. POLICE-LOG
11. CWMP
12. LED
13. LICENSING
14. USB
15. PKG_MGMT
16. SYS
17. NTP
18. SNTP
19. TIME RANGE
20. Abnormal alarm
21. USER-TASK

1 Command Line Interface

1.1alias

Configure an alias for a command.

alias mode command-alias original-command

Delete the customized command alias. For commands with default aliases, you can restore the Default Configuration.

no alias mode [command-alias]

For commands with default aliases, the Default Configuration can also be restored via default.

default alias mode [command-alias]

【Parameter Description】

Parameter	Description
mode	The Command Mode in which the command represented by the alias stands.
command-alias	Command alias.
original-command	The actual command syntax that the alias represents.

【Default Configuration】 In normal or privileged user mode, some commands have default aliases.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 The default command aliases in normal or privileged user mode are h, p, s, u, and un. The actual names are help, ping, show,

undebug, undebug.

Default command aliases cannot be removed with the no alias exec command.

By configuring command aliases, you can replace a command with a single word. For example, create an alias to represent the first part of a command, and then you can continue typing the following parts.

The Command Mode of the command represented by the alias is the Command Mode that exists in the current system. In the global configuration mode, enter alias ? to list all Command Modes that can currently configure aliases:

```
AC-FS(config)#alias ?
aaa-gs                  AAA server group mode
acl                      acl  configure  mode
bgp                      Configure bgp Protocol
config                  globle configure mode
```

Command aliases support help information, are displayed with an asterisk (*) in front of the alias, and are displayed in the following format:

*command-alias=original-command

For example, in EXEC mode, the default command alias "s" represents the "show" keyword. Then enter "s?" to get help information for keywords and aliases starting with 's':

```
AC-FS#s?
*s=show  show  start-chat  start-terminal-service
```

If the alias represents a command with more than one word, quotation marks are used to enclose the command. For example, to configure the alias "sv" in EXEC mode instead of the command show version, then:

```
AC-FS#s?
*s=show *sv="show version" show start-chat
start-terminal-service
```

Aliases must start with the first character of the command line entered, with no preceding spaces. As in the example above, if a space is entered before the command, it cannot represent a valid alias:

```
AC-FS# s?
show  start-chat  start-terminal-service
```

Command aliases can also support getting help information of the Parameter of the command. For example, the command alias "ia" in the configuration interface mode stands for "ip address", then in the interface mode:

```
AC-FS(config-if)#ia ?
A.B.C.D  IP address
dhcp     IP Address via DHCP
AC-FS(config-if)#ip address
```

The Parameter information after the ip address command is listed here, and the alias is replaced with the actual command.

Command aliases must be entered in full when they are used, otherwise they will not be recognized.

Use the show aliases command to view alias settings on your system.

【Configuration Example】 1: In the global configuration mode, use the command alias "def-route" to represent the default route setting

"ip route 0.0.0.0 0.0.0.0 192.168.1.1":

```
AC-FS#configure terminal
AC-FS(config)#alias config def-route ip route 0.0.0.0 0.0.0.0 192.168.1.1
AC-FS(config)#def-route?
*def-route="ip route 0.0.0.0 0.0.0.0 192.168.1.1" AC-
FS(config)#end
AC-FS#show aliases config
globle configure mode alias:
def-route            ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

【Verification】On the command line editing interface, configure a word as an alias for a command. Enter this word, if you can replace this command, that is, Description The alias configuration is valid.

【Prompt Information】The length of the command alias cannot exceed 19 characters. If this limit is exceeded, the following Prompt Information will appear:

```
% Overly long alias name truncated after 19 characters.
```

The length of the actual command syntax string represented by the alias cannot exceed 255 characters. If this limit is exceeded, the following Prompt Information will appear:

```
% Command alias string too long.
```

The maximum number of aliases supported in each Command Mode is 100. If this limit is exceeded, the following Prompt Information will appear:

```
% Can't add more than 100 command aliases in single mode.
```

For various unexpected reasons (such as insufficient memory, etc.), when adding an alias fails, the following Prompt Information will appear:

```
% Adding command alias fail.
```

【Common Mistake】-

【Platform Description】 -

1.2privilege

Configure the execute permission of a command to grant a command level.

privilege mode [all] {level level | reset} command-string

Restore Default Configuration.

no privilege mode [all] [level level] command-string

【Parameter Description】

Parameter	Description
mode	The CLI Command Mode to which the command it is going to authorize belongs.
all	Change the permissions of all subcommands of the specified command to the same permission level.
level level	Specifies the run permission level for the command or subcommand, the range of 0-15.
reset	Restore the execution permission for the command to the default level.
command-string	Command-string to authorize.

【Default Configuration】-

【Command Mode】 Global configuration mode

【Default Level】15

【Usage Guide】The following table shows some of the CLI Command Mode keywords that can be authorized in the privilege command. Different devices, the number of authorized Command Modes may change. In the global configuration mode, you can use privilege ? to list the current All licensable CLI Command Modes.

mode	Instruction
config	Global configuration mode.
exec	Privilege mode.
interface	Interface configuration mode.
ip-dhcp-pool	DHCP address pool configuration mode.
keychain	KeyChain configuration mode.
keychain-key	KeyChain-key configuration mode.
time-range	Time-Range Config mode.

【Configuration Example]】1: Set the password of CLI level 1 to "test", and set the permission to execute the reload command to reset the device.

```
AC-FS(config)#privilege exec level 1 reload
```

At this point, use level 1 to enter the CLI interface and find that you can use the reload command:

```
AC-FS>reload ?
LINE    Reason for reload
<cr>
```

If you want to grant all subcommands of reload to level 1 users, you can use the all keyword:

```
AC-FS(config)#privilege exec all level 1 reload
```

At this point, use level 1 to enter the CLI interface and find that all subcommands of reload can be used:

```
AC-FS>reload ?
LINE    Reason for reload
at                    reload at a specific time/date
cancel                cancel  pending  reload  scheme
in                    reload after a time interval
```

【Verification】 Select a command that is supported at a high level (eg, level 14) but not supported at a lower level (eg, level 1), and then authorize the command to the lower level. After switching to a lower level, if the command can be executed, the authorization is valid.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.3 show aliases

Displays all command aliases or command aliases under a specific Command Mode.

show aliases [mode]

【Parameter Description】

Parameter	Description
mode	The Command Mode in which the command represented by the alias stands.

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】 If Command Mode is not input, all command alias settings will be displayed.

【Configuration Example】1: Display the command alias in EXEC mode.

```
AC-FS#show aliases exec exec mode alias:
h               help
p               ping s          show
u               undebug
un              undebug
```

【Prompt Information】-

【Platform Description】 -

2 Basic configuration management

2.1 <1-99>

Resume an established Telnet Client session connection.

<1-99>

【Parameter Description】-

【Default Configuration】-

【Command Mode】 Normal user mode

【Default Level】1

【Usage Guide】 This command is used to restore the established Telnet Client session connection. When using the telnet command to initiate a Telnet Client session connection, you can use the hotkey (ctrl+shift+6 x) to temporarily exit the connection. If you need to restore the connection, you can use the number key <1-99> command to restore. At the same time, if the connection has been established, you can use the show session command to view the established connection information.

【Configuration Example]】1: Restore the established Telnet Client session connection.

```
AC-FS# 1
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.2banner exec

Customize the user login line to prompt the welcome message before entering the normal user mode.

banner exec c message c

Cancel the configuration of prompting welcome message.

no banner exec

【Parameter Description】

Parameter	Description
c	Tip the separator of the welcome information, suggesting that spacers are not allowed in the middle of the welcome information content.
message	Configuration prompt Welcome information content.

【Default Configuration】-

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to configure the welcome message. If you still enter characters after typing the ending separator, these characters will be discarded by the system.

When the user logs in to the device, MOTD (banner motd) will be displayed first, and then the Prompt Information (banner login) of LOGIN will be displayed. After the user successfully logs in to the device, the Prompt Information of EXEC (banner exec) or the incoming (banner incoming (banner incoming) will appear according to the connection type.) of the Prompt Information. If it is reverse Telnet, incoming Prompt Information will appear, and other connections will have EXEC Prompt Information. The Prompt Information configured by this command is for all line lines. If you want to prohibit EXEC Prompt Information on a line, you can configure no exec-banner on a specific line.

【Configuration Example]】1: The following example sets the welcome message:

```
AC-FS(config)# banner exec $ Welcome to Ruijie Equipment $
```

【Verification】 After configuration, the user logs into the line to enter the normal user mode, and the configured information can be displayed.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.3 banner incoming

Configure Prompt Information for Reverse Telnet Connection

banner incoming c message c

Cancel the configuration of Prompt Information for reverse telnet connection

no banner incoming

【Parameter Description】

Parameter	Description
c	Separator for Prompt Information of reverse Telnet connection. No separator is allowed in the content of Prompt Information.

【Default Configuration】-

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to configure the Prompt Information of reverse Telnet connection. If you still enter characters after typing the ending separator, these characters will be discarded by the system.

When the user logs in to the device, MOTD (banner motd) will be displayed first, and then the Prompt Information (banner login) of LOGIN will be displayed. After the user successfully logs in to the device, the Prompt Information of EXEC (banner exec) or the incoming (banner incoming) will appear according to the connection type. Prompt Information. If it is reverse Telnet, incoming Prompt Information will appear, and other connections will have EXEC Prompt Information.

【Configuration Example]】1: The following example sets the reverse Telnet connection information:

```
AC-FS(config)# banner incoming $ Welcome to Ruijie Equipment $
```

【Verification】After configuration, reverse Telnet connection user login line to enter normal user mode, and the configured information can be displayed.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.4banner login

Configure login header information

banner login c message c

Cancel the configuration of login header information

no banner login

【Parameter Description】

Parameter	Description
c	Separator for login title information, no spacer is allowed in the content of login header.
message	Configure the login title information content.

【Default Configuration】-

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to configure the login title information. If you still enter characters after typing the ending separator, these characters will be discarded by the system.

When the user logs in to the router, MOTD (banner motd) will be displayed first, and then the Prompt Information (banner login) of LOGIN will be displayed. After the user successfully logs in to the device, the Prompt Information of EXEC (banner exec) or the incoming (banner incoming) will appear according to the connection type. Prompt Information. If it is reverse Telnet, incoming Prompt Information will appear, and other connections will have EXEC Prompt Information.

【Configuration Example]】1: The following example sets the login title information:

```
AC-FS(config)# banner login $ enter your password $
```

【Verification】After configuration, the user can log in to the system to display the configured information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.5banner motd

Configure daily notification information MOTD (message of the day).

banner [motd] c message c

Cancel configuration information for daily notifications.

no banner [motd]

【Parameter Description】

Parameter	Description
c	Separator for the daily notification information, and it is not allowed in the middle of the daily notification information content.
message	Configured daily notification information content.

【Default Configuration】-

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to configure daily notification information. If characters are still input after typing the ending separator, these characters will be discarded by the system.

When the user logs in to the device, MOTD (banner motd) will be displayed first, and then the Prompt Information (banner login) of LOGIN will be displayed. After the user successfully logs in to the device, the Prompt Information of EXEC (banner exec) or the incoming (banner incoming (banner incoming) will appear according to the connection type.) of the Prompt Information. If it is reverse Telnet, incoming Prompt Information will appear, and other connections will have EXEC Prompt Information. The Prompt Information configured by this command is for all line lines. If you want to disable MOTD Prompt Information on a line, you can configure no motd-banner on a specific line.

【Configuration Example]】1: The following example sets the daily notification information:

```
AC-FS(config)# banner motd $ hello, world $
```

【Verification】After configuration, the user can log in to the system to display the configured information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.6banner privilege-mode

Configure Prompt Information for users to enter privileged mode.

banner privilege-mode c message c

Cancel the Prompt Information configuration for the user to enter the privileged mode.

no banner privilege-mode

【Parameter Description】

Parameter	Description
c	Separator for the Prompt Information in privileged mode, which is not allowed in the middle of the Prompt Information content.

【Default Configuration】-

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to configure the Prompt Information for entering the privileged mode. If you enter characters after the ending separator, these characters will be discarded by the system.

When the user enters the privileged mode, the Prompt Information (banner privilege-mode) of the privilege-mode is displayed.

【Configuration Example]】1: The following example sets the Prompt Information in privileged mode:

```
AC-FS(config)# banner privilege-mode $ Entering privilege mode! $
```

【Verification】After configuration, the configured information can be displayed when the user enters the privileged mode.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.7banner prompt-timeout

Customize Prompt Information for User Login Authentication Timeout

banner prompt-timeout c message c

Cancel user login authentication timeout prompt welcome message configuration

no banner prompt-timeout

【Parameter Description】

Parameter	Description
c	The separator that prompts the user to log in the authentication timeout information. The separator is not allowed in the content of Prompt Information.

【Default Configuration】-

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to configure the timeout information for prompting the user to log in and authenticate. If you still enter characters after typing the ending separator, these characters will be discarded by the system.

When the user's login authentication times out, the prompt-timeout Prompt Information (banner prompt-timeout) is displayed.

【Configuration Example]】1: The following example sets the login authentication timeout Prompt Information:

```
AC-FS(config)# banner exec $ login authentication timeout $
```

【Verification】After configuration, the user can log in to the line without login authentication, and the configured information can be displayed.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.8 banner slip-ppp

Custom SLIP/PPP line connection Prompt Information.

banner slip-ppp c message c

Prompt Information to cancel SLIP/PPP line connection.

no banner slip-pp

【Parameter Description】

Parameter	Description
c	Separator for Prompt Information. No separator is allowed in the content of Prompt Information.

【Default Configuration】-

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to configure the welcome message. If you still enter characters after typing the ending separator, these characters will be discarded by the system.

When connected via a SLIP/PPP line (such as a router dial-up connection), the corresponding terminal will display slip-ppp Prompt Information (banner slip-ppp).

【Configuration Example]】1: The following example sets the SLIP/PPP Prompt Information:

```
AC-FS(config)# banner slip-ppp $ Welcome to Ruijie Equipment $
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.9 configure

Enter global configuration mode.

configure [terminal]

【Parameter Description】-

【Default Configuration】-

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Enter global configuration mode.

```
AC-FS# configure
AC-FS(config)#
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.10debug support

Enter diagnostic mode.

debug support

【Parameter Description】-

【Default Configuration】-

【Command Mode】 Privileged user mode

【Default Level】15

【Usage Guide】 Use this command to enter diagnostic mode from privileged user mode.

【Configuration Example]】1: Enter debug support mode.

```
AC-FS# debug support
%Warning: Enter debug support mode, all commands in this mode are used to diagnose system hardware and software.
          Misuse of these commands will affect system performance. Therefore, use these commands under the guidance of AC-FS Networks engineers.

AC-FS(support)#
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.11 disable

Decrease the level of the current user.

disable [privilege-level]

【Parameter Description】

Parameter	Description
privilege-level	Permission level.

【Default Configuration】-

【Command Mode】 Normal user mode

【Default Level】 0

【Usage Guide】 Use this command to exit from privileged user mode to normal user mode. If the permission level is added, the current permission level is lowered to the specified permission level.

The permission level following the disable command must be lower than the current permission level.

【Configuration Example]】1: The following example configures the device to lower the current permission level to level 10:

```
AC-FS# disable 10
```

【Verification】Use the show privilege command to view the level of the current user.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.12disconnect

Disconnect pending Telnet Client connections.

disconnect session-id

【Parameter Description】

Parameter	Description
session-id	Suspended Telnet Client connection session number.

【Default Configuration】-

【Command Mode】 Normal user mode

【Default Level】1

【Usage Guide】 Disconnect the specified Telnet Client by entering the specified Telnet Client connection session number.

【Configuration Example】1: Enter the specified Telnet Client connection session number and disconnect the specified Telnet Client connection.

```
AC-FS# disconnect 1
```

【Verification】1: Use the show sessions command to check whether the specified Telnet Client connection has been disconnected.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.13 do telnet

Log in to the Telnet server.

do telnet

【Parameter Description】-

【Default Configuration】-

【Command Mode】 Normal user mode | Privileged mode | Interface mode

【Default Level】1

【Usage Guide】-

【Configuration Example】-

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.14enable

Enter privileged user mode.

enable [privilege-level]

【Parameter Description】

Parameter	Description
privilege-level	Permission level.

【Default Configuration】-

【Command Mode】 Normal user mode

【Default Level】 0

【Usage Guide】 Use this command to enter from normal user mode to privileged user mode. If the permission level is added, the current permission level will be upgraded to the specified permission level.

【Configuration Example]】1: The following example configures the device to reduce the current permission level to level 14:

```
AC-FS> enable 14
  Password:
```

【Verification】Use the show privilege command to view the level of the current user.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.15enable password

Configure passwords for different privilege levels.

enable password [level level] { [0] password | 7 encrypted-password }

Deletes the password for the specified level.

no enable password [level level]

【Parameter Description】

Parameter	Description
level	Permissions level of the user.
0	(Optional) Specify a plaintext password string.
password	Clear password of the user entering the privileged EXEC configuration layer, string length range: 1~126.
7 encrypted-password	The password string entered is a ciphertext string.

【Default Configuration】-

【Command Mode】 Global configuration mode

【Default Level】15

【Usage Guide】 Usually it is not necessary to enter the encryption type. Typically, the encryption type is only required when copying and pasting a password encrypted by the device. Valid passwords are defined as follows:

Must contain 1 to 26 uppercase and lowercase alphanumeric characters.

Leading spaces can be preceded by the password, but are ignored. Intermediate and trailing spaces are part of the password.

If you specify an encryption type and then enter a clear text password, you cannot re-enter privileged EXEC mode. It cannot be recovered by any means.

Encrypted lost password, only the device password can be reconfigured.

【Configuration Example]】1: The following example sets the password to pw10:

```
AC-FS(config)# enable password pw10
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.16enable secret

Configure secure passwords for different privilege levels.

enable secret [level level] { [0] password | 5 encrypted-secret }

Deletes the password for the specified level.

no enable secret [level level]

【Parameter Description】

Parameter	Description
level	The user's level.
0	(Optional) Specify a plaintext password string.
password	Clear password of the user entering the privileged EXEC configuration layer, string length range: 1~126.
5 encrypted-password	Specifies the password text of MD5 and is configured as the encrypted password to save.

【Default Configuration】-

【Command Mode】 Global configuration mode

【Default Level】15

【Usage Guide】 Enable authentication password is divided into password and security password: password is a simple encrypted password, which can only be set to level 15 password;

The security password is a security encryption password, which can be set for levels 0 to 15.

If the above two passwords exist at the same level in the system, the password password will not take effect. If a non-level 15 password is set, a warning prompt will be given, and it will be automatically converted to the security password; if the level 15 password and the security password are set to be exactly the same, a warning prompt will be given; the password must be stored in encrypted form, The password password uses simple encryption, and the security password uses secure encryption.

【Configuration Example]】1: The following example sets the security password to pw10:

```
AC-FS(config)# enable secret 0 pw10
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.17 enable service

Turn on and off the specified service (SSH Server/Telnet Server/Web Server/Snmp Agent).

enable service { ssh-server | telnet-server | web-server [http | https | all] | snmp-agent }

【Parameter Description】

Parameter	Description
ssh-server	Open and close the SSH Server, and the command opens both the IPv4 and IPv6 services.
telnet-server	Open and close the Telnet Server, and the command opens both the IPv4 and IPv6 services.
web-server [http | https | all]	Open and close the Web Server, and the command opens both the IPv4 and IPv6 services.
snmp-agent	Open and close the Snmp Agent, and the command opens both the IPv4 and IPv6 services.

【Default Configuration】 By default, telnet-server, snmp-agent and web-server are enabled, and ssh-server is disabled.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command is used to open and close the specified service. Use the no enable service command to turn off the specified service.

The enable service web-server command is followed by 3 optional keywords [http | https | all]. If the command is executed without any keyword, or followed by the all keyword, it means that both http service and https service are opened; if it is followed by the http keyword, it means that only the http service is opened; if it is followed by the https keyword, it means that only Open https service.

【Configuration Example]】1: The following example command enable service ssh-server enables the SSH Server function:

```
AC-FS(Config)# enable service ssh-server
```

【Verification】View the open or close status of the service through the show service command

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.18end

Exit from configuration mode to privileged mode

end

【Parameter Description】-

【Default Configuration】-

【Command Mode】All unprivileged modes

【Default Level】 0

【Usage Guide】 In any unprivileged mode, just execute the end command to exit to the privileged mode

【Configuration Example]】1: The following example command end exits to privileged mode:

```
AC-FS#con
Enter configuration commands, one per line. End with CNTL/Z. AC-
FS(config)#line vty 0
AC-FS(config-line)#end
*May 20 09:49:38: %SYS-5-CONFIG_I: Configured from console by console
AC-FS#
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.19 exec-banner

Reactivate the display of EXEC Prompt Information on the specified line

exec-banner

Suppress the display of EXEC Prompt Information on the specified line

no exec-banner

【Parameter Description】-

【Default Configuration】Activate EXEC Prompt Information on all lines.

【Command Mode】 LINE configuration mode

【Default Level】 14

【Usage Guide】If banner exec and banner motd are configured, EXEC and MOTD Prompt Information will be displayed on all lines by default. If you want to close EXEC and MOTD Prompt Information on a specific line, you can use the no form of this command to close EXEC and MOTD Prompt Information on the specified line.

This command has no effect on banner incoming, that is, if banner incoming is configured, the reverse Telnet on all lines.

The incoming Prompt Information is displayed in the connection, and the incoming Prompt Information cannot be turned off on the specified line.

【Configuration Example]】1: The following example displays the welcome message for line 1 prohibition:

```
AC-FS(config)# line vty 1
AC-FS(config-line)no exec-banner
```

【Verification】After configuration, the user logs in to the system, and the configured information is not displayed.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.20exec-timeout

Configure the connection timeout to this device under LINE.

exec-timeout minutes [seconds]

Cancel the connection timeout under LINE, the connection never times out.

no exec-timeout

【Parameter Description】

Parameter	Description
minutes	The number of minutes for the specified timeout, with a value range of 0-35791.
seconds	(Optional) Number of seconds specified for the timeout, with a value range of 0-2147483.

【Default Configuration】 The default timeout time is 10 minutes

【Command Mode】 LINE configuration mode

【Default Level】 14

【Usage Guide】 If this connection does not have any input or output information within the specified time, the connection will be interrupted and the LINE will be restored to an idle available state.

【Configuration Example]】1: The following example specifies that the connection timeout for line vty 0 is 5 minutes and 30 seconds:

```
AC-FS(config-line)# exec-timeout 5 30
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.21execute

Execute commands in a batch file.

execute { [flash:] filename }

【Parameter Description】

Parameter	Description
filename	File path required to execute.

【Default Configuration】 Non-configuration command

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Read the string line by line from the file and execute it.

【Configuration Example】】 1: The following example shows an example of using the execute command to configure the specified interface ip:

```
AC-FS#execute flash:mybin/config.text
executing script file mybin/config.text .....
executing done
```

```
AC-FS#config
Enter configuration commands, one per line. End with CNTL/Z. AC-
FS(config)#interface gigabitEthernet 0/1
AC-FS(config-if-GigabitEthernet 0/1)#ip address 192.168.21.158 24
AC-FS(config-if-GigabitEthernet 0/1)#end
*Sep 29 23:35:49: %SYS-5-CONFIG_I: Configured from console by console
AC-FS#
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】-

【Platform Description】 -

2.22exit

Exit from configuration mode to superior mode or exit CLI interface from privileged mode

exit

【Parameter Description】-

【Default Configuration】-

【Command Mode】 All modes

【Default Level】 0

【Usage Guide】-

【Configuration Example]】1: The following example command exit exits to the superior mode:

```
AC-FS#con
Enter configuration commands, one per line. End with CNTL/Z. AC-
FS(config)#line vty 0
AC-FS(config-line)#end
*May 20 09:49:38: %SYS-5-CONFIG_I: Configured from console by console
AC-FS#con
Enter configuration commands, one per line. End with CNTL/Z. AC-
FS(config)#line vty 0
AC-FS(config-line)#exit AC-
FS(config)#exit
*May 20 09:51:48: %SYS-5-CONFIG_I: Configured from console by console AC-
FS#exit


Press RETURN to get started
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.23 help

Check out the help system for some brief information.

help

【Parameter Description】-

【Default Configuration】-

【Command Mode】Any configuration mode

【Default Level】1

【Usage Guide】Use this command to view some brief descriptions of the help system. During the specific configuration process, you can use "?" to view all commands in the current configuration mode or the Parameter type that follows a command.

【Configuration Example]】1: The following example only displays some brief information about the help system:

```
AC-FS#help
Help may be requested at any point in a command by entering
a question mark '?'.  If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)
```

2: The following example shows all commands that can be run in interface configuration mode:

```
AC-FS(config-if-GigabitEthernet 0/0)#?
Interface configuration commands:
  arp              ARP interface subcommands
  bandwidth        Set bandwidth informational parameter
  carrier-delay    Specify delay for interface transitions
  dampening        Enable event dampening
  default          Set a command to its defaults
  description      Interface specific description
  dldp             Exec data link detection command
```

```
  duplex           Configure duplex operation
  efm              Config efm for an interface
  end              Exit from interface configuration mode
  exit             Exit from interface configuration mode
  expert           Expert extended ACL
  flowcontrol      Set the flow-control value for an interface
  full-duplex      Force full duplex operation
  global           Global ACL
  gvrp             GVRP configure command
  half-duplex      Force half duplex operation
  help             Description of the interactive help system
  ip               Interface Internet Protocol config commands
  ipv6             Internet Protocol Version 6
  isis             Intermediate System - Intermediate System (IS-IS)
  l2               Config L2 attribute
  label-switching  Enable interface process mpls packet
  lacp             LACP interface subcommands
  lldp             Link Layer Discovery Protocol
  load-interval    Specify interval for load calculation for an interface
  mac              Mac extended ACL
  mac-address      Set mac-address
  mpls             Multi-Protocol Label Switching
  mtu              Set the interface Maximum Transmission Unit (MTU)
  no               Negate a command or set its defaults
  ntp              Configure NTP
  port-group       Aggregateport/port bundling configuration
  redirect         Redirect packets
  rmon             Rmon command
  security         Configure the Security
  show             Show running system information
  shutdown         Shutdown the selected interface
  snmp             Modify SNMP interface parameters
  speed            Configure speed operation
  switchport       Set switching mode characteristics
  vrf              Multi-af VPN Routing/Forwarding parameters on the interface
  vrrp             VRRP interface subcommands
  xconnect         Xconnect commands
```

3: The following example shows the type of Parameter that follows the command:

```
AC-FS(config)#access-list 1 permit ?
  A.B.C.D  Source address
```

```
any      Any source host
host     A single source host
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.24hostname

Specifies or modifies the hostname of the device.

hostname name

【Parameter Description】

Parameter	Description
name	The hostname of the device. Only strings, numbers, and connectors can be used. The maximum length is 63 characters.

【Default Configuration】 The default host name is AC-FS.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 The host name is mainly used to identify the device and as the user name of the local device in dial-up and CHAP authentication.

【Configuration Example]】1: The following example specifies the hostname of the device as BeiJing_AC-FS:

```
AC-FS(config)# hostname BeiJing_AC-FS
BeiJing_AC-FS(config)#
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.25ip telnet source-interface

Specifies the IP address on the interface as the source address for Telnet connections.

ip telnet source-interface interface-name

【Parameter Description】

Parameter	Description
interface-name	Specify the IP address configured on this interface as the source address of Telnet connection. Interface types include AP port, Gi port, Loopback port, null port, Tunnel port, and VLAN port.

【Default Configuration】-

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command is used to specify the IP address on the interface as the source address of the global Telnet connection. When using the telnet command to log in to a Telnet server, if no source interface or source address is specified separately for the connection, this global setting will be used.

Use the no ip telnet source-interface command to restore the setting to the default value.

【Configuration Example]】1: The following example command specifies the IP address on the Loopback 1 interface as the source address of the global Telnet connection:

```
AC-FS(config)# ip telnet source-interface Loopback 1
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.26lock

Set a temporary password on the terminal.

lock

【Parameter Description】-

【Default Configuration】-

【Command Mode】 Normal user mode

【Default Level】1

【Usage Guide】 By setting a temporary password, the user keeps the connection session and locks the terminal interface to prevent access. Lock the terminal interface by following these steps:

1. The first point: enter the lock command, the system will prompt for a password;

2. The second point: enter the password, which can be any string. After entering, the system will prompt to confirm the entered password, then the system will clear the screen and display the "Locked" message;

3. To re-enter the terminal, you need to enter the set temporary password.

To use the terminal locking feature on a terminal, you need to turn on the feature that supports locking the terminal on the corresponding line by executing the lockable command in line configuration mode.

【Configuration Example]】1: The following example locks a terminal interface:

```
AC-FS(config-line)# lockable
AC-FS(config-line)# end AC-FS#
lock
Password: <password>
Again: <password>
Locked
Password: <password>
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.27 lockable

Allows the user to lock the terminal connected to the current line.

lockable

Cancel the setting.

no lockable

【Parameter Description】-

【Default Configuration】 The terminal does not support the lock command by default.

【Command Mode】 LINE configuration mode

【Default Level】1

【Usage Guide】 This command is used to support the feature of locking the terminal on the corresponding line. To lock the terminal, you can execute the lock command in EXEC mode.

If the user wants to execute the lock command to lock the terminal connected to the current line, he must first use the command lockable to set the current line to allow the user to lock the terminal connected to the current line.

【Configuration Example】】1: The following example enables the function of locking the terminal on the console port and locks the console:

```
AC-FS(config)# line console 0
AC-FS(config-line)# lockable
AC-FS(config-line)# end AC-FS#
lock
Password: <password>
Again: <password>
Locked
Password: <password>
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.28 login

Configure simple login password verification on the LINE line with AAA turned off.

login

Cancel login password verification.

no login

【Parameter Description】-

【Default Configuration】 The console disables the login function by default, and the VTY terminal enables the login function by default.

【Command Mode】 LINE configuration mode

【Default Level】 14

【Usage Guide】 If the AAA security service is not enabled, this command is used for simple password verification during login authentication. The password here refers to the password configured in the VTY or console interface.

【Configuration Example]】1: The following example demonstrates setting up login password verification on VTY.

```
AC-FS(config)# no aaa new-model AC-
FS(config)# line vty 0
AC-FS(config-line)# password 0 normatest
AC-FS(config-line)# login
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.29 login authentication

With AAA turned on, configure a list of login authentication methods on the LINE line.

login authentication { default | list-name }

Delete the login authentication method list.

no login authentication { default | list-name }

【Parameter Description】

Parameter	Description
default	Default authentication method list name.
list-name	Default authentication method list name.

【Default Configuration】 When AAA is enabled, the default authentication method is used.

【Command Mode】 LINE configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】】 1: The following example demonstrates how to associate a method list on VTY and use radius for login authentication.

```
AC-FS(config)# aaa new-model
AC-FS(config)# aaa authentication login default group radius AC-
FS(config)# line vty 0
AC-FS(config-line)# login authentication default
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.30login local

Configure local user authentication on the LINE line with AAA turned off.

login local

Cancel the login local user authentication.

no login local

【Parameter Description】-

【Default Configuration】-

【Command Mode】 LINE configuration mode

【Default Level】 14

【Usage Guide】 If the AAA security service is not enabled, this command is used to configure the local user authentication when LINE line login authentication is performed. The local user here refers to the user information configured through the username command.

【Configuration Example]】1: The following example demonstrates setting up login local authentication on VTY.

```
AC-FS(config)# no aaa new-model AC-FS(config)#
username test password 0 test AC-FS(config)#
line vty 0
AC-FS(config-line)# login local
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.31 login privilege log

When the privilege level of the terminal user is elevated, the corresponding log information is output.

login privilege log

Cancel the output of Prompt Information when the user privilege level is elevated.

no login privilege log

【Parameter Description】-

【Default Configuration】 This function is disabled by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 If you need to monitor terminal user privilege level elevation, you need to configure this function, which is valid for all terminals.

【Configuration Example]】1: The following example demonstrates opening the prompt function of user privilege level elevation.

```
AC-FS(config)# login privilege log
```

2: The following example demonstrates the log information displayed when the user fails to change the permission level after enabling this function.

```
AC-FS>enable 10
  Password:
Password:
Password:


% Access denied
AC-FS>
*Sep 10 11:34:19: %SYS-5-PRIV_AUTH_FAIL: Authentication to privilege level 10 from console failed
```

3: The following example demonstrates the log information that is prompted when the user fails to change the permission level after enabling this function.

```
AC-FS>enable 10
  Password: AC-
FS#
*Sep 10 11:34:20: %SYS-5-PRIV_AUTH_SUCCESS: Authentication to privilege level 10 from console success
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.32motd-banner

Reactivate the display of MOTD Prompt Information on the specified line

motd-banner

Suppress the display of MOTD Prompt Information on the specified line

no motd-banner

【Parameter Description】-

【Default Configuration】 Activate MOTD Prompt Information on all lines.

【Command Mode】 LINE configuration mode

【Default Level】 14

【Usage Guide】 If banner exec and banner motd are configured, EXEC and MOTD Prompt Information will be displayed on all lines by default. If you want to close EXEC and MOTD Prompt Information on a specific line, you can use the no form of this command to close EXEC and MOTD Prompt Information on the specified line.

This command has no effect on banner incoming, that is, if banner incoming is configured, reverse Telnet on all lines.

The incoming Prompt Information is displayed in the connection, and the incoming Prompt Information cannot be turned off on the specified line.

【Configuration Example]】 1: The following example displays the MOTD information that the Vty1 line is disabled:

```
AC-FS(config)# line vty 1
AC-FS(config-line)no motd-banner
```

【Verification】 After configuration, the user logs in to the system, and the configured information is not displayed.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

2.33password

Configure the line line login password.

password { [0] password | 7 encrypted-password }

Delete the line login password.

no password

【Parameter Description】

Parameter	Description
0	(Optional) Specify a plaintext password string.
password	Specifies the clear password for the remote user line line, string length range: 1~25.
7 encrypted-password	The password string entered is a ciphertext string.

【Default Configuration】 -

【Command Mode】 LINE configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: The following example specifies the line login password as red:

```
AC-FS(config)# line vty 0
AC-FS(config-line)# password red
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.34prompt

Prompt for configuring the user command interface (CLI).

prompt string

Unconfigure the user command interface (CLI) prompt.

no prompt

【Parameter Description】

Parameter	Description
string	Command prompt string with up to 32 characters.

【Default Configuration】-

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 If you do not configure the prompt of the command interface (CLI), the system name is used as the prompt, and the prompt will change with the change of the system name. The command interface (CLI) prompt is only valid in EXEC mode.

【Configuration Example]】1: The following example will configure the command prompt as FSOS:

```
AC-FS(config)# prompt FSOS AC-
FS(config)# end
FSOS
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.35secret

Configure the line line login MD5 irreversible encrypted password.

secret { [0] password | 5 encrypted-secret }

Delete line line login MD5 irreversible encrypted password.

no secret

【Parameter Description】

Parameter	Description
0	(Optional) Specify the explicit password text for MD5 irreversible encryption.
password	Specifies the clear password for the remote user line line, string length: 1~25.
5 encrypted-secret	Specifies the password text of MD5 and is configured as the encrypted password to save.

【Default Configuration】-

【Command Mode】line configuration mode

【Default Level】 14

【Usage Guide】 This command is used to configure the MD5 irreversible encrypted password to authenticate the remote user trying to

log in to the line.

If the specified encryption type is 5, the legal ciphertext length must be 24, and the 1st, 3rd, and 8th characters of the password text must be "$" characters.

It is usually not necessary to specify an encryption type of 5. Normally, you only need to specify an encryption type of 5 when copying and pasting an encrypted password.

The password and secret password can be configured at the same time under the line. When the password and secret password are configured on the system, when the user enters the password when logging in, the secret password will be preferentially matched. If the secret password fails to match, it will continue to match the password password. If all passwords fail to match, the user fails to log in.

【Configuration Example】 The following example specifies that the line login MD5 irreversible encryption password is vty0:

```
AC-FS(config)# line vty 0
AC-FS(config-line)# secret vty0
```

After configuring this password, vty0 will perform MD5 irreversible encryption, and the effect of show is as follows:

```
secret 5 $1$X834$wvx6y794uAD8svzD
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

2.36 session-timeout

Configures the timeout period for sessions established on the current LINE to the remote terminal.

session-timeout minutes [output]

Cancel the timeout period of the session down LINE to the remote terminal, the session never times out.

no session-timeout

【Parameter Description】

Parameter	Description
minutes	The number of minutes for the specified timeout time.

output	Whether the output data is also input to determine whether the timeout.

【Default Configuration】 The default timeout time is 0 min, which means it will never timeout.

【Command Mode】 LINE configuration mode

【Default Level】 14

【Usage Guide】If there is no input or output information from the session that has been established on the current LINE to the remote terminal within the specified time, the connection will be interrupted and the LINE will be restored to the idle available state.

【Configuration Example]】1: The following example specifies the session timeout for line vty 0 to be 5 minutes:

```
AC-FS(config-line)# session-timeout 5 output
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.37 show debugging

Displays the debug switch on information of the current device.

show debugging

【Parameter Description】-

【Command Mode】 Privileged user mode

【Default Level】15

【Usage Guide】-

【Configuration Example]】1: The following example is an example of executing the show debugging command:

```
AC-FS#show debugging

debug fw-group detect intf-state
```

【Prompt Information】-

2.38 show hostname

Display the hostname information of the current device.

show hostname

【Parameter Description】-

【Command Mode】 Privileged user mode

【Default Level】15

【Usage Guide】-

【Configuration Example]】1: The following example is an example of executing the show hostname command, the example shows that the host name of the device is AC-FS:

```
AC-FS#show hostname AC-
FS
AC-FS#
```

【Prompt Information】-

【Platform Description】 -

2.39 show line

View the configuration information of the line.

show line { console line-num | vty line-num | line-num }

【Parameter Description】

Parameter	Description
console	View the configuration information of the console line

vty	View the configuration information of the virtual terminal line.
line-num	The line to view.

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example]】 1: View the configuration information of the console port.

```
AC-FS# show line console 0
CON      Type    speed   Overruns
* 0      CON     9600    45927
Line 0, Location: "", Type: "vt100"
Length: 24 lines, Width: 79 columns
Special Chars: Escape  Disconnect  Activation
               ^^x    none     ^M
Timeouts:  Idle EXEC  Idle Session
              never        never
```

```
History is enabled, history size is 10.
Total input: 53564 bytes
Total output: 395756 bytes
Data overflow:  27697 bytes
stop rx interrupt:  0 times
```

Field Description:

Parameter	Description
CON	Terminal type, CON means console. 0 means the terminal line number, plus * in front of the number means The terminal currently in use.
Type	Terminal type, including CON, VTY, etc.
speed	Asynchronous rate.
Overruns	The statistical value of the number of overrun errors received by the driver.
Line 0	Terminal line number.
Location: ""	Line location setting.
Type: "vt100"	The line is compatible with terminal standards.

Special Chars	Terminal special characters, including Escape characters, Disconnect characters, and Activation characters.
Timeouts	Terminal timeout time, never means never timeout.
History	History command record switch and maximum number of entries.
Total input	Statistics of the amount of data received from the driver.
Total output	Statistics of the amount of data sent to the drive.
Data overflow	Receive overflowed data volume statistics.
stop rx interrupt	Drives the statistical value of the number of RX interrupts.

【Prompt Information】-

【Platform Description】 -

2.40show reload

Check your system's restart settings.

show reload

【Parameter Description】-

【Command Mode】 Privileged user mode

【Default Level】1

【Usage Guide】

【Configuration Example]】1: The following example shows the settings for system restart:

```
AC-FS# show reload
System reload state: Warm
```

Field Description:

Field	Instruction
System reload state	Status of system restart

【Prompt Information】-

【Platform Description】 -

2.41 show running-config

View the running configuration information of the current device system or the configuration information under an interface.

show running-config [interface interface]

【Parameter Description】-

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】-

【Prompt Information】-

【Platform Description】 -

2.42show service

View the current service's on or off status.

show service

【Parameter Description】-

【Command Mode】 Privileged user mode

【Default Level】1

【Usage Guide】-

【Configuration Example]】1: View the current service's on or off status.

```
AC-FS# show service web-
server  : disabled
web-server(https): disabled
snmp-agent : enabled ssh-
server  : enabled
telnet-server : disabled
```

【Prompt Information】-

【Platform Description】 -

2.43 show sessions

Displays information about each instance of the Telnet Client instance that has been established.

show sessions

【Parameter Description】-

【Command Mode】 Normal user mode

【Default Level】1

【Usage Guide】 Displays the information of each instance of the established Telnet Client instance, including: the VTY number occupied by the connection and the server address.

【Configuration Example】1: Display the connection information of the established Telnet Client session.

```
AC-FS#show sessions
Conn  Address
*1    127.0.0.1
*2    192.168.21.122
```

【Prompt Information】-

【Platform Description】 -

2.44 show startup-config

View the configuration of the device stored on NVRAM (Non-Volatile Random Access Memory).

show startup-config

【Parameter Description】-

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】 The configuration of the device stored in NVRAM (Non-Volatile Random Access Memory), that is, startup-config is the configuration executed when the device is started.

On FS devices, startup-config refers to the configuration information saved in the default configuration file "/config.text" in the built-in Flash of the device.

【Configuration Example】-

【Prompt Information】-

【Platform Description】 -

2.45show this

View the configuration information that takes effect in the current system mode.

show this

【Parameter Description】-

【Command Mode】 All configuration modes

【Default Level】 14

【Usage Guide】 The configuration of the current mode will not be displayed in the range mode. include:

1. Specify and configure a range of lines through the line first-line last-line command, and enter the LINE configuration mode;

2. Specify and configure multiple VLANs through the vlan range command, and enter the vlan range configuration mode;

3. Specify and configure multiple interfaces through the interface range command, and enter the interface range configuration mode;

In the above case, the configuration information that takes effect in the current mode cannot be displayed when this command is used. If

this command is executed, the displayed configuration is empty.

【Configuration Example]】 1: The following example shows the configuration information that takes effect under interface fastEthernet 0/1

```
AC-FS (config)#interface fastEthernet 0/1 AC-
FS (config-if-FastEthernet 0/1)#show this
Building configuration...
 !
 spanning-tree link-type point-to-point
 spanning-tree mst 0 port-priority 0
 !
end
AC-FS (config-if-FastEthernet 0/1)#
```

【Prompt Information】 -

【Platform Description】 -

2.46speed

Configure the rate of the end device.

speed speed

Restore the default configuration of the end device rate.

no speed

【Parameter Description】

Parameter	Description
speed	The transmission rate of the terminal device, in bps. For the serial interface, the transmission rate can only be set to one of 9600, 19200, 38400, 57600, 115200, and the default rate is 9600.

【Default Configuration】 The default rate is 9600.

【Command Mode】 LINE configuration mode

【Default Level】 14

【Usage Guide】 Users can set the baud rate of the asynchronous line according to their needs. The command speed will set both the receive rate and the transmit rate of the asynchronous line.

【Configuration Example】1: The following example sets the serial port rate to 57600 bps:

```
AC-FS(config)# line console 0
AC-FS(config-line)# speed 57600
```

【Verification】Use the show line command to view the rate configured by the LINE line.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.47telnet

Log in to the Telnet server.

telnet host [port] [/source { ip A.B.C.D | ipv6 X:X:X:X::X | interface interface-name }]

【Parameter Description】

Parameter	Description
host	The IPV4 address, IPV6 address or host name of the Telnet server.
port	The TCP port number of the Telnet server, the default value is 23.
/source	Specify the source IP or source interface used by the Telnet client.
ip A.B.C.D	Specify the source IPV4 address used by the Telnet client.
ipv6 X:X:X:X::X	Specify the source IPV6 address used by the Telnet client.
interface interface-name	Specify the source interface used by the Telnet client.

【Default Configuration】-

【Command Mode】 Normal user mode

【Default Level】1

【Usage Guide】-

【Configuration Example]】1: In the following example, the destination device IPV4 address of telnet is 192.168.1.1, the port uses the default value, and the specified source interface is Gi 0/1.

```
AC-FS# telnet 192.168.1.1 /source interface gigabitEthernet 0/1
```

2: In the following example, the destination device IPV6 address of telnet is 2AAA:BBBB::CCCC

```
AC-FS# telnet 2AAA:BBBB::CCCC
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.48username

Configure the local user account and optional authorization information.

username name [login mode { console | ssh | telnet }] [online amount number] [permission oper-mode path] [privilege privilege-level] [reject remote-login] [web-auth] [pwd-modify] [nopassword | password [0 | 7] text-string]

Delete local users.

no username name

【Parameter Description】

Parameter	Description
name	username.
login mode	Configure the account login method restriction.
console	The login method of the restricted account is console.
ssh	The login method of the restricted account is ssh.
telnet	The login method for restricted accounts is telnet.
online amount number	Configure the number of accounts online at the same time.
permission oper-mode path	Configure the account's operation authority for the specified file, op-mode indicates the

	operation mode, and path indicates the path of the file or directory.
privilege privilege-level	Configure the permission level of the account, the value range is 0-15.
reject remote-login	Restrict the use of this account to log in remotely.
web-auth	This account can only be used for web authentication.
pwd-modify	Allow web authentication users using this account to change their passwords. This option is only available after web-auth is configured.
nopassword	No password is configured for this account.
password [0 | 7] text-string	Configure the password of the account, 0 means to enter a plain text password, 7 means to enter a cipher text password, the default is to enter a plain text password.

【Default Configuration】-

【Command Mode】 Global configuration mode

【Default Level】15

【Usage Guide】 This command is used to create a local user database for authentication.

If the specified encryption type is 7, the legal ciphertext length entered must be an even number.

It is usually not necessary to specify an encryption type of 7. In general, you only need to specify encryption type 7 when copying and pasting an encrypted password.

【Configuration Example]】1: The following example configures a user name and password, and binds the user level to level 15:

```
AC-FS(config)# username test privilege 15 password 0 pw15
```

2: The following example configures a dedicated username and password for web authentication:

```
AC-FS(config)# username user1 web-auth password 0 pw
```

3: The following example configures the user test to have read and write permissions to all files and directories:

```
AC-FS(config)# username test permission rw /
```

4: The following example configures the user test to have read, write, and execute permissions on other files and directories except the config.text file:

```
AC-FS(config)# username test permission n /config.text
AC-FS(config)# username test permission rwx /
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.49 username import

Import user information from a file.

username import filename

【Parameter Description】

Parameter	Description
filename	file name.

【Default Configuration】-

【Command Mode】 Privileged user mode

【Default Level】1

【Usage Guide】 This command is used to import user information from outside.

【Configuration Example]】1: The following example configuration imports user information:

```
AC-FS# username import user.csv
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.50username export

Export user information to a file.

username export filename

【Parameter Description】

Parameter	Description
filename	file name.

【Default Configuration】-

【Command Mode】 Privileged user mode

【Default Level】1

【Usage Guide】 This command is used to export user information to a file.

【Configuration Example]】1: The following example configuration imports user information:

```
AC-FS# username export user.csv
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2.51write

Save the system configuration (running-config) to the specified location.

write [memory | terminal]

【Parameter Description】

Parameter	Description
memory	Writing the system configuration into NVRAM is equivalent to copy running-config

	startup-config.
terminal	Display system configuration, which is equivalent to show running-config.

【Default Configuration】-

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】Although this command has an alternative command, it is still reserved for the convenience of users due to its wide use and recognition.

If the device where the file is located exists, the system will automatically create the specified file and write the system configuration; if the device where the file is located does not exist (possibly: the startup configuration file is specified in a USB flash drive or SD card, etc. on a removable storage device that has not been loaded when the write [memory] command is executed), the system will ask whether to save the current configuration in the default startup configuration file "/config.text", and according to the user's Answer Take the appropriate action.

【Configuration Example]】1: The following demonstrates how to save the system configuration on the device:

```
AC-FS# write
Building configuration...
[OK]
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3 LINE

3.1 access-class

Control terminal login via ACL filtering (IPv4).

access-class { access-list-number | access-list-name } { in | out }

Cancel ACL filtering (IPV4) to control terminal login.

no access-class { access-list-number | access-list-name } { in | out }

【Parameter Description】

Parameter	Description
access-list-number	ACL number, configurable range: IP standard ACL (1-99, 1300-1999); IP extended ACL (100-199, 2000-2699).
access-list-name	ACL name.
in	Filter the incoming connections.
out	Filter outgoing connections.

【Default Configuration】-

【Command Mode】 LINE configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure ACL number 20 to filter incoming connections from VTYs in the range of 0-5.

```
AC-FS(config)# line vty 0 5
AC-FS(config-line)#access-class 20 in
```

2: Configure ACL filtering with the ACL name of test on the outgoing connections of VTYs with numbers ranging from 6 to 7.

```
AC-FS(config)# line vty 6 7
AC-FS(config-line)#access-class test out
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.2accounting commands

Enables the accounting of command activities on the line line.

accounting commands level { default | list-name }

Cancels the command activity accounting function.

no accounting commands level

【Parameter Description】

Parameter	Description
level	The command level of accounting, the range is 0~15. When deciding which level of command is executed, information needs to be recorded.
default	The name of the default authentication method list.
list-name	Optional method list name.

【Default Configuration】 Turn off the accounting function on the line.

【Command Mode】 LINE configuration mode

【Default Level】 14

【Usage Guide】Used in conjunction with AAA authentication, first configure the AAA command accounting method, and then apply it to the terminal line that needs command accounting.

【Configuration Example]】1: Enable the command activity accounting function on the Vty 1 line, and the command level required for accounting is level 15.

```
AC-FS(config)# aaa new-model
AC-FS(config)# aaa accounting commands 15 default start-stop group tacacs+ AC-
FS(config)# line vty 1
AC-FS(config-line)# accounting commands 15 default
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.3accounting exec

Enables user access activity accounting on line.

accounting exec { default | list-name }

Cancel the Exec accounting function.

no accounting exec

【Parameter Description】

Parameter	Description
default	Default authentication method list name.
list-name	Optional method list name.

【Default Configuration】Close the accounting function on the line

【Command Mode】 LINE configuration mode

【Default Level】 14

【Usage Guide】Used in conjunction with AAA authentication, first configure the AAA Exec accounting method, and then apply it to the terminal line that needs to perform Exec accounting.

【Configuration Example]】1: Enable the Vty 1 line user access activity accounting function.

```
AC-FS(config)# aaa new-model
AC-FS(config)# aaa accounting exec default start-stop group radius AC-
FS(config)# line vty 1
AC-FS(config-line)# accounting exec default
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.4authorization commands

Enable command authorization on the line.

authorization commands level { default | list-name }

Cancel the command authorization function.

no authorization commands level

【Parameter Description】

Parameter	Description
level	The command level to be authorized, ranging from 0 to 15, determines which level of command needs to be authorized before it can be executed.
default	Default authentication method list name.
list-name	Optional method list name.

【Default Configuration】 Disable the command authorization function.

【Command Mode】 LINE configuration mode

【Default Level】 14

【Usage Guide】Used in conjunction with AAA authentication, first configure the AAA command authorization method, and then apply it to the terminal line that needs command authorization.

【Configuration Example]】1: Authorize the level 15 commands executed by users on the Vty 1 line.

```
AC-FS(config)# aaa new-model
AC-FS(config)# aaa authorization commands 15 default group tacacs+ AC-
FS(config)# line vty 1
AC-FS(config-line)# authorization commands 15 default
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.5authorization exec

Turn on the Exec authorization feature on the line.

authorization exec { default | list-name }

Cancel the Exec authorization function.

no authorization exec

【Parameter Description】

Parameter	Description
default	Default authentication method list name.
list-name	Optional method list name.

【Default Configuration】 Disable the Exec authorization function.

【Command Mode】 LINE configuration mode

【Default Level】 14

【Usage Guide】Used in conjunction with AAA authentication, first configure the AAA Exc authorization method, and then apply it to the terminal line that needs Exec authorization.

【Configuration Example]】1: Exec authorization for Vty 1 line.

```
AC-FS(config)# aaa new-model
AC-FS(config)# aaa authorization exec default group radius AC-
FS(config)# line vty 1
AC-FS(config-line)# authorization exec default
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.6 clear line

Clears the connection status of the line.

clear line { console line-num | vty line-num | line-num }

【Parameter Description】

Parameter	Description
console	Clear the connection status of the console line.
vty	Clear the connection status of the virtual terminal line.
line-num	Cleared line.

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】 Use the clear line command to clear the connection status of the line, which will forcibly disconnect the connected terminal. And restore the line to the unoccupied state, the terminal connection can be re-established.

【Configuration Example]】1: Clear the connection status of LINE VTY 13. If there is already a client (such as Telnet, SSH, etc.) connection session on this VTY, it will immediately disconnect.

```
AC-FS# clear line vty 13
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.7disconnect-character

Sets a hotkey for disconnecting Terminal Services.

disconnect-character ascii-value

Restore default default settings.

no disconnect-character

【Parameter Description】

Parameter	Description
ascii-value	The decimal value corresponding to the ASCII code of the hot key to disconnect the terminal service connection, the value range is 0-255.

【Default Configuration】 By default, the system sets the hotkey for terminal service disconnection as Ctrl+D, which is the key combination corresponding to 0x04.

【Command Mode】 LINE configuration mode

【Default Level】 14

【Usage Guide】 This command sets the hot key for disconnecting the terminal service connection. Users can set the hot key for disconnecting the terminal service connection according to their needs. The terminal service disconnection hotkey cannot be a common ASCII code (such as 'a'~'z', 'A'~'Z' and '0'~'9', etc.), otherwise, the terminal service will not be able to communicate normally.

【Configuration Example]】1: Set the hotkey for disconnecting terminal services on Vty0-5 to Ctrl+E (its ASCII value is 0x05).

```
AC-FS(config)# line vty 0 5
AC-FS(config-line)# disconnect-character 5
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.8escape-character

Sets the exit character on the line.

escape-character escape-value

Restore system default settings.

no escape-character

【Parameter Description】

Parameter	Description
escape-value	The decimal value corresponding to the ASCII code of the user-defined exit character, the value range is 0-255.

【Default Configuration】 By default, the escape character has been set on the line and its escape-value is 30, that is, Ctrl+^ (the key combination is Ctrl+Shift+6).

【Command Mode】 LINE configuration mode

【Default Level】 14

【Usage Guide】 If the escape-character escape-value command is set, the user can use the key combination corresponding to escape-value and then type "x" to interrupt the current session and return to the original session that created the session.

【Configuration Example]】1: Set the exit character on the Vty 0 line to 23 (the corresponding key combination is (Ctrl+w)).

```
AC-FS(config)# line vty 0
AC-FS(config-line)# escape-character 23
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.9exec

Allow the line line to enter the command line interface.

exec

Restricts the line line to the command line interface.

no exec

【Parameter Description】-

【Default Configuration】 By default, the line is allowed to enter the command line interface.

【Command Mode】 LINE configuration mode

【Default Level】 14

【Usage Guide】If the line line is not allowed to enter the command line interface, you can configure no exec, then the user cannot enter the command line interface through the configured line when logging in, but enters the command line interface through other unrestricted lines.

【Configuration Example】1: Limit 1 line to enter the command line interface.

```
AC-FS(config)# line vty 1 AC-
FS(config-line)# no exec AC-
FS# show users
Line             User         Host(s)              Idle       Location
──────────────── ──────────── ──────────────────── ────────── ────────────────────
*  0 con 0       ---          idle                 00:00:00 -------
   1 vty 0       ---          idle                 00:01:03   20.1.1.2
   3 vty 2       ---          idle                 00:00:13   20.1.1.2
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.10history

Enable the line history command recording function, or configure the number of entries recorded by the line history command.

history [size size]

Cancel the line history command record function.

no history

Restore the number of entries recorded by the line history command.

no history size

【Parameter Description】

Parameter	Description
size size	Number of entries, value range: 0~256.

【Default Configuration】 By default, the history command record function is enabled, and the maximum number of entries in the history command record is 10

【Command Mode】 LINE configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the number of history records for line 0-5 to be 20.

```
AC-FS(config)# line vty 0 5
AC-FS(config-line)# history size 20
```

2: Turn off the history record function of line 0-5.

```
AC-FS(config)# line vty 0 5
AC-FS(config-line)# no history
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.11ipv6 access-class

Control terminal login via ACL filtering (IPv6).

ipv6 access-class access-list-name { in | out }

Cancel control terminal login via ACL filtering (IPv6).

no ipv6 access-class access-list-name { in | out }

in Filter incoming connections.

out Filter outgoing connections.

【Parameter Description】

Parameter	Description
access-list-name	ACL name.
in	Filter incoming connections.
out	Filter outgoing connections.

【Default Configuration】-

【Command Mode】 LINE configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the ACL filtering with the ACL name test for the IPv6 connections outgoing from the VTY with the number range of 0-4.

```
AC-FS(config)# line vty 0 4
AC-FS(config-line)#ipv6 access-class test out
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.12length

Sets the maximum number of lines per screen on the specified line termination.

length screen-length

Restore default settings.

no length

【Parameter Description】

Parameter	Description
screen-ength	Row height value, the value range is 0-512.

【Default Configuration】 By default, the maximum number of lines on a single screen is 24 lines.

【Command Mode】 LINE configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Set the maximum number of lines on a single screen of the specified line to 10 lines.

```
AC-FS(config-line)# length 10
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.13line

Enter the specified LINE mode.

line [console | vty] first-line [last-line]

【Parameter Description】

Parameter	Description
console	Console port.
vty	Virtual terminal line, suitable for Telnet or SSH connection.
first-line	The number of the first-line to enter.
last-line	The last-line number to be entered.

【Default Configuration】-

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Enter the LINE mode of LINE VTY 1 to 3.

```
AC-FS(config)# line vty 1 3
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.14line vty

Increase the number of VTY connections currently available.

line vty line-number

Reduce the number of VTY connections currently available.

no line vty line-number

【Parameter Description】

Parameter	Description
line-number	Number of VTY connections, range: 0~35.

【Default Configuration】-

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Increase the number of available VTY connections to 20, and the range of available VTY numbers is 0-19.

```
AC-FS(config)# line vty 19
```

2: Reduce the number of available VTY connections to 10, the range of available VTY numbers is 0-9.

```
AC-FS(config)# no line vty 10
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.15location

Set the location Description of the specified line.

location location

Restore system default settings.

no location

【Parameter Description】

Parameter	Description
location	Description of the location of the current route.

【Default Configuration】-

【Command Mode】 LINE configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Set the location Description of the specified line to Swtich's Line Vty 0.

```
AC-FS(config)# line vty 0
AC-FS(config-line)# location Swtich's Line Vty 0
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.16monitor

Supports turning on log display on the terminal.

monitor

Cancel opening the log display on the terminal.

no monitor

【Parameter Description】-

【Default Configuration】-

【Command Mode】 LINE configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Support the terminal printing log on the line 0-5.

```
AC-FS(config)# line vty 0 5
AC-FS(config-line)# monitor
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.17privilege level

Configure the line login level.

privilege level level

Restore line login level.

no privilege level

【Parameter Description】

Parameter	Description
level	Permission level, the value range is 0-15.

【Default Configuration】 By default, the privilege level is 1.

【Command Mode】 LINE configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Set the login permission level of VTY line 0-4 to 14.

```
AC-FS(config)# line vty 0 4
AC-FS(config-line)#privilege level 14
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.18refuse-message

Configure the line line to refuse to log in Prompt Information.

refuse-message [c message c]

Cancel the line line to refuse to log in Prompt Information.

no refuse-message

【Parameter Description】

Parameter	Description
c	Separator for refusing to log in Prompt Information, and no separator is allowed in the content of Prompt Information that refuses to log in.

【Default Configuration】-

【Command Mode】 LINE configuration mode

【Default Level】 14

【Usage Guide】Use this command to configure the logout prompt information. If you still enter characters after typing the end delimiter, these characters will be discarded by the system. When the user is denied login to the device, the window will prompt the current line to deny the user login Prompt Information.

【Configuration Example]】1: Configure the line logout prompt information to restrict illegal users from logging in to Ruijie devices.

AC-FS(config-line)#refuse-message @ Illegal users are restricted from logging in to FS devices @

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.19 show history

Displays the history commands for the current line.

show history

【Parameter Description】-

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】Display the history commands recorded by the current line.

```
AC-FS# show history
exec:
sh privilege
sh run
show user
sh user all
show history
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.20show line

View the configuration information of the line.

show line { console line-num | vty line-num | line-num }

【Parameter Description】

Parameter	Description
console	Check the configuration information of the console line.
vty	Check the configuration information of the virtual terminal line.
line-num	Check the line.

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: View the configuration information of the console port.

```
AC-FS# show line console 0
CON      Type    speed   Overruns
* 0      CON     9600    45927
Line 0, Location: "", Type: "vt100"
Length: 24 lines, Width: 79 columns
Special Chars: Escape  Disconnect  Activation
               ^^x    none     ^M
Timeouts:  Idle EXEC  Idle Session
              never        never
History is enabled, history size is 10.
Total input: 53564 bytes
Total output:  395756 bytes
Data overflow: 27697 bytes
stop rx interrupt:  0 times
```

Field Description:

Field	Instruction
CON	Terminal type, CON means console. 0 means the terminal line number, and the number before the * sign means the terminal being used before.
Type	Terminal type, including CON, AUX, TTY, VTY, etc.
speed	Asynchronous rate.
Overruns	The statistical value of the number of overrun errors received by the driver.
Line 0	Terminal line number.
Location: ""	Line location setting.
Type: "vt100"	The line is compatible with terminal standards.
Special Chars	Terminal special characters, including Escape characters, Disconnect characters, and Activation characters.
Timeouts	Terminal timeout time, never means never timeout.
History	History command record switch and maximum number of entries.
Total input	Statistics of the amount of data received from the driver.
Total output	Statistics of the amount of data sent to the drive.
Data overflow	Receive overflowed data volume statistics.
stop rx interrupt	Drives the statistical value of the RX interrupt quantity.

【Prompt Information】-

【Platform Description】 -

3.21show privilege

Displays the current line permission level.

show privilege

【Parameter Description】-

【Command Mode】 Privileged user mode

【Default Level】1

【Usage Guide】-

【Configuration Example】Display the current line permission level.

```
AC-FS# show privilege
Current privilege level is 10
```

【Prompt Information】-

【Platform Description】 -

3.22 show users

Display line login user information.

show users [all]

【Parameter Description】

Parameter	Description
all	Display the information of all log-in line users, including the information of the currently logged-in line users and the information of the unlogged-in line users.

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Display the information of currently logged in line users.

```
AC-FS# show users
Line              User         Host(s)              Idle       Location
──────────────── ──────────── ──────────────────── ────────── ──────────────────
   0 con 0        ---          idle                 00:00:46 -------
   1 vty 0        ---          idle                 00:00:29   20.1.1.2
*  2 vty 1        ---          idle                 00:00:00   20.1.1.2
```

2: Display all line user information.

```
AC-FS(config)# show users all
Line              User         Host(s)              Idle       Location
──────────────── ──────────── ──────────────────── ────────── ──────────────────
   0 con 0        ---          idle                 00:00:49 -------
   1 vty 0        ---          idle                 00:00:32   20.1.1.2
*  2 vty 1        ---          idle                 00:00:00   20.1.1.2
   3 vty 2        ---                               00:00:00 -------
   4 vty 3        ---                               00:00:00 -------
   5 vty 4        ---                               00:00:00 -------
   6 vty 5        ---                               00:00:00 -------
```

【Prompt Information】-

【Platform Description】 -

3.23speed

Sets the baud rate on the specified line termination.

speed baudrate

Restore default settings.

no speed

【Parameter Description】

Parameter	Description
baudrate	The baud rate value, the range is 9600-115200.

【Default Configuration】 By default, the baud rate is 9600.

【Command Mode】 LINE configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Set the baud rate of the specified line to 115200.

```
AC-FS(config-line)# speed 115200
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.24 terminal escape-character

Sets the exit character for the current terminal.

terminal escape-character escape-value

Restore the system default settings of the current terminal.

terminal no escape-character

【Parameter Description】

Parameter	Description
escape-value	The decimal value corresponding to the ASCII code of the user-defined exit character, the value range is 0-255.

【Default Configuration】 By default, the escape character has been set on the line and its escape-value is 30, that is, Ctrl+^ (the key combination is Ctrl+Shift+6).

【Command Mode】 Privileged user mode

【Default Level】 14

【 Usage Guide 】If the escape-character escape-value command is set, the user can use the key combination corresponding to escape-value and then type "x" to interrupt the current session and return to the original session that created the session.

【Configuration Example】1: Set the exit character of the current terminal to 23 (the corresponding key combination is (Ctrl+w)).

```
AC-FS# terminal escape-character 23
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.25 terminal history

Enable the line history command record function in the current terminal, or configure the number of entries in the line history command record.

terminal history [size size]

Cancel the line history command recording function in the current terminal.

terminal no history

The number of entries recorded by the line history command to restore at the current terminal

terminal no history size

【Parameter Description】

Parameter	Description
size size	Number of entries, value range: 0~256.

【Default Configuration】By default, the history command record function is enabled, and the maximum number of entries in the history command record is 10.

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Set the number of history records of the current terminal's line to 20.

```
AC-FS# terminal history size 20
```

2: Turn off the history record function of the line line of the current terminal.

```
AC-FS# terminal no history
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.26 terminal length

Sets the maximum number of lines per screen on the current terminal.

terminal length screen-length

Restore the default settings of the current terminal.

terminal no length

【Parameter Description】

Parameter	Description
screen-engtth	Row height value, the range is 0-512.

【Default Configuration】 By default, the maximum number of lines on a single screen is 24 lines.

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Set the maximum number of lines in a single screen of the current terminal to 10 lines.

```
AC-FS# terminal length 10
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.27 terminal location

Set the current terminal location Description.

terminal location location

Restore the system default settings of the current terminal.

terminal no location

【Parameter Description】

Parameter	Description
location	The location of the current route description.

【Default Configuration】-

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Set the current terminal location Description to Swtich's Line Vty 0.

```
AC-FS# terminal location Swtich's Line Vty 0
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.28 terminal speed

Set the baud rate on the current terminal.

terminal speed baudrate

Restore default settings.

terminal no speed

【Parameter Description】

Parameter	Description
baudrate	Baud rate value, the value range is 9600-115200.

【Default Configuration】 By default, the baud rate is 9600.

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Set the baud rate of the current terminal to 115200.

```
AC-FS# terminal speed 115200
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.29 terminal width

Configure the maximum number of columns in a single line on the current terminal, that is, the width of a line.

terminal width screen-width

Restore the line width of the current terminal.

terminal no width

【Parameter Description】

Parameter	Description
screen-width	The row width value, the range is 0-256.

【Default Configuration】 By default, the maximum number of columns in a single row is 79.

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】 -

【Configuration Example】 1: Set the maximum number of columns in a single row of the current terminal to 10.

```
AC-FS# terminal width 10
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

3.30timeout login

Set the line login authentication timeout time.

timeout login response seconds

Restore the default line login authentication time.

no timeout login response

【Parameter Description】

Parameter	Description
response	Line is the time to wait for the user to enter any information.
seconds	Timeout time, the value range is 1-300, and the unit is second.

【Default Configuration】 The timeout time for authentication waiting for user input, the default is 30 seconds.

【Command Mode】 LINE configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】Configure the login authentication timeout for line Vty lines 0-5 to 300 seconds.

```
AC-FS(config)# line vty 0 5
AC-FS(config-line)#timeout login response 300
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.31transport input

Specifies the protocol that can communicate under the line.

transport input { all | ssh | telnet | none }

Restore the protocols that can be communicated under the line.

no transport input { all | ssh | telnet | none }

【Parameter Description】

Parameter	Description
all	Allow all agreements.
ssh	Allow ssh protocol.
telenet	Allow telnet protocol.
none	No agreement is allowed.

【Default Configuration】 By default, the protocols that can be communicated are all, that is, both ssh and telnet protocols are available.

【Command Mode】 LINE configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】The VTY line of configuration 0-4 only allows telnet communication protocol.

```
AC-FS(config)# line vty 0 5
AC-FS(config-line)#transport input ssh
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.32vacant-message

Configure the line line to log out of Prompt Information.

vacant-message [c message c]

Cancel the line line to log out of Prompt Information.

no vacant-message

【Parameter Description】

Parameter	Description
c	The separator of Prompt Information when logging out, and the separator is not allowed in the content of Prompt Information when logging out.
message	Log out of Prompt Information.

【Default Configuration】-

【Command Mode】 LINE configuration mode

【Default Level】 14

【Usage Guide】 Use this command to configure the logout prompt information. If you still enter characters after typing the ending separator, these characters will be discarded by the system. When the user logs out of the device, the window will prompt the current line to log out of the Prompt Information.

【Configuration Example]】1: Configure the line line to log out and log out Prompt Information to log out of FS device.

```
AC-FS(config-line)#vacant-message @ Quit FS device @
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.33width

Configures the maximum number of columns on a single line on the specified line termination, that is, the width of a line.

width screen-width

Restore the line width of the specified line.

no width

【Parameter Description】

Parameter	Description
screen-width	Line width value, the value range is 0-256.

【Default Configuration】 By default, the maximum number of columns in a single row is 79.

【Command Mode】 LINE configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Set the maximum number of columns in a single row of the specified line to 10.

```
AC-FS(config-line)# width 10
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

4 RMON

4.1rmon alarm

Configure the RMON alarm function.

rmon alarm number variable interval {absolute | delta} rising-threshold value [event-number]

falling-threshold value [event-number] [owner ownername]

Deletes the specified alarm entry.

no rmon alarm number

【Parameter Description】

Parameter	Description
number	The index number of the alarm entry, the limit range: 1~65535
variable	The alarm variable is a string of 1 to 255 characters and is expressed in dotted format of the node OID (the format is entry.integer.instance, such as 1.3.6.1.2.1.2.1.10.1)
Interval	Sampling interval time, the unit is second, the value range is 1～2147483647
absolute	The sampling type is absolute value sampling, that is, the value of the variable is directly extracted when the sampling time is reached
delta	The sampling type is variable value sampling, that is, when the sampling time is reached, the variable value of the variable in the sampling interval is extracted
rising-threshold value	Set the upper limit of the number of samples Parameter value, the value range: -2147483648~+2147483647
event-number	(Optional) Trigger an event with event number event-number when the upper and lower limits are reached
falling-threshold value	Set the lower limit of the number of samples Parameter value, the value range: -2147483648~+2147483647
owner ownername	(Optional) Set the ownername of the creator of the entry, the ownername is a string of 1 to 63 characters, case sensitive

【Default Configuration】-

【Command Mode】 Global mode

【Default Level】 14

【**Usage Guide**】Allows you to modify the parameters of the configured alarm entries, including the alarm variable, sampling type, creator of the entry, sampling interval, upper/lower limit of the number of samples and their corresponding trigger events.

【**Configuration Example]**】1: Monitor the MIB variable instance ifInNUcastPkts.6, the sampling interval is 60 seconds, when the sampling value reaches the upper limit of 20 or the lower limit of 10, event 1 will be triggered for event processing.

```
AC-FS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AC-FS(config)# rmon alarm 10 1.3.6.1.2.1.2.2.1.12.6 60 delta rising-threshold 20 1 falling-threshold
10 1 owner UserA
```

【**Verification**】1: Use the show run command to check whether the command configuration is successful.

2: Use the show rmon alarm or show rmon command to view the specific Parameter content of the alarm table entry.

【**Prompt Information**】 1: When deleting a configuration that does not exist, it will prompt an error.

2: When the upper threshold is less than or equal to the lower threshold, an error will be prompted.

3: If the input OID of the monitored object is unreasonable, an error will be prompted.

4: When the number of configuration entries has reached the upper limit and no further configuration is allowed, an error will be displayed.

5: If the memory application is unsuccessful, an error will be displayed.

【**Common Mistake**】 1: The OID of the input monitored object is unreasonable, the variable corresponding to the OID does not exist or the type is not an integer or an unsigned integer.

2: The upper limit threshold is less than or equal to the lower limit threshold

【**Platform Description**】 -

4.2rmon collection history

Configure the historical statistics function of the Ethernet interface.

rmon collection history index [owner ownername] [buckets bucket-number] [interval seconds]

Deletes the specified historical information entry.

no rmon collection history index

【**Parameter Description**】

Parameter	Description

index	Index number of history control table entry, value range: 1~65535.
owner ownername	(Optional) Set the ownername of the creator of the entry, the ownername is a string of 1 to 63 characters, case sensitive.
buckets bucket-number	(Optional) Set the capacity of the history statistics table corresponding to the history control table entry, that is, set the maximum number of records that the history statistics table can hold. bucket-number, bucket-number value range: 1~65535, the default value is 10.
interval seconds	(Optional) Set the statistical period value seconds, the unit is seconds, the value range of seconds: 1~3600, the default value is 1800s.

【Default Configuration】-

【Command Mode】 Interface mode

【Default Level】 14

【Usage Guide】It is not allowed to modify the Parameter of the configured history control table entry; it is not allowed to delete the history statistics entry that is not configured on the interface under the interface.

【Configuration Example]】1. Configure to use the historical statistics function on port GigabitEthernet 0/1, set the size of the historical statistics table to 5, and the statistics period to 60s.

```
AC-FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z. AC-
FS(config)#interface gigabitEthernet 0/1
AC-FS(config-GigabitEthernet0/1)#rmon history 1 owner UserA buckets 5 interval 60
```

【Verification】1: Use the show run command to check whether the command configuration is successful.

2: Use the show rmon history or show rmon command to view the history control table and the specific parameter content of the generated history statistics table entries.

【Prompt Information】 1: When deleting a configuration that does not exist, it will prompt an error.

2: Modify the configured history control table entry Parameter, prompting an error.

3: When the number of configuration entries has reached the upper limit and no more configuration is allowed, an error is displayed.

4: In the case of unsuccessful application of memory, an error will be prompted.

【Common Mistake】 1: Repeat the configuration or modify the already configured history control table entries.

【Platform Description】 -

4.3rmon collection stats

Configure the Ethernet interface statistics function.

rmon collection stats index [owner ownername]

Deletes the specified Ethernet interface statistics entry.

no rmon collection stats index

【Parameter Description】

Parameter	Description
index	The index number of the statistical table item, the value range: 1~65535.
owner ownername	(Optional) Set the ownername of the creator of the entry. The ownername is a string of 1 to 63 characters, case sensitive, and spaces are not supported.

【Default Configuration】-

【Command Mode】 Interface mode

【Default Level】 14

【Usage Guide】It is not allowed to modify the Parameter of the configured statistics table entry; it is not allowed to delete the historical statistics table entries that are not configured on the interface under the interface.

【Configuration Example]】1: Configure to use the statistics function on port GigabitEthernet 0/1.

```
AC-FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z. AC-
FS(config)#interface gigabitEthernet 0/1
AC-FS(config-GigabitEthernet0/1)# rmon stats 1 owner UserA
```

【Verification】1: Use the show run command to check whether the command configuration is successful.

2: Use the show rmon statistics or show rmon command to view the specific Parameter content of the statistics table entry.

【Prompt Information】 1: When deleting a configuration that does not exist, it will prompt an error.

2: Modify the configured statistics table item Parameter, prompting an error.

3: When the number of configuration entries has reached the upper limit and no more configuration is allowed, an error is displayed.

4: In the case of unsuccessful application of memory, an error will be prompted.

【Common Mistake】 1: Repeat the configuration or modify the already configured statistics table entries.

【Platform Description】 -

4.4rmon event

Configure RMON events.

rmon event number [log] [trap community] [description description-string] [owner ownername]

Deletes the specified event table entry.

no rmon event number

【Parameter Description】

Parameter	Description
number	Index number of the event table, value range: 1~65535.
log	(Optional) Log events. When an event is triggered, the system will record a log. The default log record capacity is 10, and the oldest record will be deleted when it exceeds 10.
trap community	(Optional) Trap event, when the event is triggered, the system will send Trap with community as the community name.
description description-string	(Optional) Set the description information description-string of the event, description-string is a string of 1 to 127 characters.
owner ownername	(Optional) Set the ownername of the entry creator, which is a string of 1 to 63 characters, case sensitive.

【Default Configuration】-

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Allows to modify the parameters of the configured event table item, including the event table type, community name, creator, description information and other parameters.

【Configuration Example]】1: Define the action of the event: record the event, send the trap message, the community name used for trap sending is public.

```
AC-FS#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AC-FS(config)#rmon event 1 log trap public description "ifInNUcastPkts is abnormal" owner UserA
```

【Verification】1: Use the show run command to check whether the command configuration is successful.

2: Use the show rmon event or show rmon command to view the event table and the specific Parameter content of the generated event record table entry.

【Prompt Information】 1: When deleting a configuration that does not exist, it will prompt an error.

2: When the number of configuration entries has reached the upper limit and no more configuration is allowed, an error is displayed.

3: In the case of unsuccessful application for memory, an error will be prompted.

【Common Mistake】-

【Platform Description】 -

4.5 show rmon

Displays all RMON information.

show rmon

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Display information includes all alarm table information, event table and event record table information, history control table and history record table information, statistics table information.

【Configuration Example】

```
AC-FS#show   rmon
ether statistic table:
                    index = 1
                    interface = GigabitEthernet 0/1
                    owner = admin
                    status = 0
```

```
                    dropEvents = 61
                    octets = 170647461
                    pkts = 580375
                    broadcastPkts = 2135
                    multiPkts = 3615
                    crcAlignErrors = 0
                    underSizePkts = 0
                    overSizePkts = 0
                    fragments = 0
                    jabbers = 0
                    collisions = 0
                    packets640ctets = 3254668
                    packets65To1270ctets = 1833370
                    packets128To2550ctets = 2098146
                    packets256To5110ctets = 126716
                    packets512To10230ctets = 363621
                    packets1024To15180ctets = 1077865

rmon history control table:
                    index = 1
                    interface = GigabitEthernet 0/1
                    bucketsRequested = 5
                    bucketsGranted = 5
                    interval = 60
                    owner = UserA
                    stats = 1

rmon history table:
                    index = 1
                    sampleIndex = 2485
                    intervalStart = 7d:22h:56m:38s
                    dropEvents = 0
                    octets = 5840
                    pkts = 27
                    broadcastPkts = 0
                    multiPkts = 0
                    crcAlignErrors = 0
                    underSizePkts = 0
                    overSizePkts = 0
                    fragments = 0
                    jabbers = 0
```

```
collisions = 0
 utilization = 0
//There are 4 more historical records information ignored here
rmon alarm table:
 index: 1
  interval: 60
 oid = 1.3.6.1.2.1.2.2.1.12.6
 ampleType: 2
 alarmValue: 0
 startupAlarm: 3
  risingThreshold: 20
fallingThreshold: 10
 risingEventIndex: 1
fallingEventIndex: 1
 owner: UserA
  status: 1

rmon event table:
 index = 1
 description = ifInNUcastPkts is abnormal
 type = 4
 community = public
 lastTimeSent = 0d:0h:0m:0s
 owner =UserA
status = 1
rmon log table:
 eventIndex = 1
 index = 1
  logTime = 6 d:19 h:21 m:48 s
logDescription = ifInNUcastPkts is abnormal
```

【Prompt Information】-

【Platform Description】 -

4.6show rmon alarm

Displays the alarm table information.

show rmon alarm

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: View the alarm table information.

```
AC-FS#show rmon alarm
rmon alarm table:
                  index: 1
                  interval: 60
                  oid = 1.3.6.1.2.1.2.2.1.12.6
                  sampleType: 2
                  alarmValue: 0
                  startupAlarm: 3
                  risingThreshold: 20
                  fallingThreshold: 10
                  risingEventIndex: 1
                  fallingEventIndex: 1
                  owner: UserA
                  status: 1
```

【Prompt Information】-

【Platform Description】 -

4.7 show rmon event

Display event table information

show rmon event

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: View event table information.

```
AC-FS#show rmon event
rmon event table:
                    index = 1
                    description = ifInNUcastPkts is abnormal
                    type = 4
                    community = public
                    lastTimeSent = 0d:0h:0m:0s
                    owner =UserA
                    status = 1

rmon log table:
                    eventIndex = 1
                    index = 1
                    logTime = 6d:19h:21m:48s
                    logDescription = ifInNUcastPkts is abnormal
```

【Prompt Information】-

【Platform Description】 -

4.8 show rmon history

Display history table information.

show rmon history

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: View historical group information.

```
AC-FS#show rmon history
rmon history control table:
```

```
                    index = 1
                    interface = GigabitEthernet 0/1
                    bucketsRequested = 5
                    bucketsGranted = 5
                    interval = 60
                    owner = UserA
                    stats = 1

rmon history table:
                    index = 1
                    sampleIndex = 2485
                    intervalStart = 7d:22h:56m:38s
                    dropEvents = 0
                    octets = 5840
                    pkts = 27
                    broadcastPkts = 0
                    multiPkts = 0
                    crcAlignErrors = 0
                    underSizePkts = 0
                    overSizePkts = 0
                    fragments = 0
                    jabbers = 0
                    collisions = 0
                    utilization = 0
```

// There are 4 more history information to ignore here

【Prompt Information】-

【Platform Description】 -

4.9 show rmon statistics

Display Ethernet statistics.

show rmon statistics

【Parameter Description】

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: View Ethernet statistics.

```
AC-FS#show rmon statistics
ether statistic table:
                  index = 1
                  interface = GigabitEthernet 0/1
                  owner = admin
                  status = 0
                  dropEvents = 61
                  octets = 170647461
                  pkts = 580375
                  broadcastPkts = 2135
                  multiPkts = 3615
                  crcAlignErrors = 0
                  underSizePkts = 0
                  overSizePkts = 0
                  fragments = 0
                  jabbers = 0
                  collisions = 0
                  packets64Octets = 3254668
                  packets65To127Octets = 1833370
                  packets128To255Octets = 2098146
                  packets256To511Octets = 126716
                  packets512To1023Octets = 363621
                  packets1024To1518Octets = 1077865
```

【Prompt Information】-

【Platform Description】 -

5 File System

5.1cd

Change the current path or file system.

cd [filesystem:] [directory]

【Parameter Description】

Parameter	Description
filesystem:	The url of the file system is followed by a colon. Possible file systems include: flash:, usb:, tmp:.
directory	The path name, if it starts with "/", it means an absolute path, otherwise it means a relative path.

【Default Configuration】 The default file system is flash:, if the path name is not specified, it means the root path of the file system.

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】-

【Configuration Example】-

【Verification】Change and view the current working path through cd and pwd commands.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

5.2copy

Copy files between file systems.

copy src-url dst-url

【Parameter Description】

Parameter	Description
src-url	The URL of the source file of the copy action. The source file can be local or remote.
dst-url	The URL of the destination file of the copy action. The destination file can be local or remote.

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】When the file to be copied already exists on the target URL, the target file system decides what to do, such as reporting an error, overwriting, or letting the user choose.

The url can be in the following format:

Parameter Description:

Parameter	Description
running-config	The current configuration file that is running.
startup-config	Configuration file used for initialization.
flash:	Local flash file system.
tftp:	The URL of the TFTP network server, the syntax is as follows:tftp:[[//location]/directory]/filename.
xmodem:	Files on network devices using xmodem protocol.

【Configuration Example]】1: Copy the file netconfig on the 192.168.64.2 device to the netconfig of the flash disk, the local netconfig already exists:

```
AC-FS#copy tftp://192.168.64.2/netconfig flash:/netconfig
The file [flash:/netconfig] exits,override it? [Y/N]: y
Copying: !!!!!!!!

Accessing tftp://192.168.64.2/netconfig finished, 2399bytes prepared
Flushing data to flash:/netconfig...
Flush data done
```

【Verification】Copy and display file information through the copy and dir commands.

【Prompt Information】-

【Common Mistake】 The specified copy source file is a directory, and a directory cannot be copied.

【Platform Description】 -

5.3delete

Delete a file.

delete [filesystem:] file-url [/force | /recursive]

【Parameter Description】

Parameter	Description
filesystem:	The url of the file system, followed with a colon, and possible file systems include: flash:, usb:, tmp:.
file-url	A file name with a path, if starting with "/", indicates the absolute path, or otherwise the relative path.
/force	Force file deletion without waiting for user confirmation.
/recursive	Recursively delete all the files of a directory, including the directory itself.

【Default Configuration】 The default file system is flash:.

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】-

【Configuration Example]】1: Delete the file fstab on the flash disk:

```
AC-FS#pwd
flash:/ AC-
FS#dir
Directory of flash:/
1------rw-         336    Jan 03 2012 18:53:42  fstab
2------rw-        4096    Jan 03 2012 12:32:09  rc.d
3------rw-    10485760    Jan 03 2012 18:13:37  rpmdb
3 files, 0 directories
10,490,192 bytes total (13,192,656 bytes free) AC-
FS#delete flash:/fstab
AC-FS#dir
Directory of flash:/
1------rw-        4096    Jan 03 2012 12:32:09  rc.d
2------rw-    10485760    Jan 03 2012 18:13:37  rpmdb
2 files, 0 directories
10,489,856 bytes total (13,192,992 bytes free)
```

2: Recursively delete the non-empty folder file on the flash disk:

```
AC-FS#pwd
flash:/ AC-
FS#dir
Directory of flash:/
   1 drwx             0  Thu Jan  1 02:02:25 1970  file
   2 -rw-        610019  Tue Aug 14 02:21:13 2012  file-5.11.tar.gz
1 file, 1 directory
58,720,256 bytes total (28,577,792 bytes free)
AC-FS#delete /recursive flash:/file
```

```
AC-FS#dir
Directory of flash:/
   1 -rw-        610019  Tue Aug 14 02:21:13 2012  file-5.11.tar.gz
1 file, 0 directories
58,720,256 bytes total (31,358,976 bytes free)
```

【Verification】 Delete files through delete and dir commands and display file information.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.4dir

Displays a list of files on a file system.

dir [filesystem:] [file-url]

【Parameter Description】

Parameter	Description
filesystem:	The url of the file system, followed with a colon, and possible file systems include: flash:, usb:, tmp:.
file-url	Path name, if starting with "/", indicates the absolute path, otherwise the relative path.

【Default Configuration】 The default file system is flash:, if the path name is not specified, it means the root path of the file system.

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】-

【Configuration Example]】1: Display the file list of the root directory of the flash disk:

```
AC-FS#dir flash:/
Directory of flash:/
1------rw-        336    Jan 03 2012 18:53:42  fstab
2------rw-       4096    Jan 03 2012 12:32:09  rc.d
3------rw-   10485760    Jan 03 2012 18:13:37  rpmdb
3 files, 0 directories
10,490,192 bytes total (13,192,656 bytes free)
```

Field Description:

Field	Description
1、2、3.。。。	reference number.
-rw-	Permissions, a file can have any of the following items: The d: indicates that this is a directory. r: readable w: Can write x: performability

10485760	file size .
rpmdb	document name.
files	Number of documents statistics.
directories	Catalog number statistics.
total	Total size.
free	The remaining available space.

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

5.5 eject

Unmount the USB device

eject [usb0]

【Parameter Description】-

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】15

【Usage Guide】-

【Configuration Example】1: Uninstall the USB device:

```
AC-FS#eject ?
  sd0   Eject sd disk 0
  usb0  Eject usb disk 0
```

【Verification】You can view it with show mount after eject

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

5.6erase

Erase a device or file without a file system.

erase filesystem:

【Parameter Description】

Parameter	Description
filesystem:	File system name, followed by a colon.

【Default Configuration】

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】-

【Configuration Example]】1: Erase usb file system:

```
AC-FS#erase usb0:
Sure to erase usb0:? [Y/N] y
Erasing disk usb0 ...
Erase disk usb0 done!
```

【Verification】Use dir command to view file information after erase.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

5.7file

Display information about a file.

file [filesystem:] file-url

【Parameter Description】

Parameter	Description
filesystem:	The url of the file system is followed with a colon, and possible file systems include: flash:, sata:, usb:, sd:,tmp:.
file-url	A file name with a path, if starting with "/", indicates the absolute path, or otherwise the relative path.

【Default Configuration】 The default file system is flash:.

【Command Mode】 Privileged mode

【Default Level】15

【Usage Guide】-

【Configuration Example]】1: Display the information of the gcc executable file:

```
AC-FS#file flash:/gcc
/usr/bin/gcc-4.6: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked (uses shared libs), for GNU/Linux 2.6.15, stripped
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

5.8 file prompt

Specifies the level of prompting.

file prompt [noisy | quiet]

noisy confirms all file operations.

quiet rarely prompts

【Parameter Description】

Parameter	Description
noisy	Confirm it for all file operations.
quiet	Very few hints.

【Default Configuration】 noisy

【Command Mode】 Privileged mode

【Default Level】15

【Usage Guide】-

【Configuration Example]】1: Modify the file prompt level to noisy mode:

```
AC-FS#file prompt noisy
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

5.9mkdir

Create a new directory.

mkdir [filesystem:] directory

【Parameter Description】

Parameter	Description
filesystem:	The url of the file system, followed with a colon, and possible file systems include: flash:, usb:, tmp:.
directory	Path name, if starting with "/", indicates the absolute path, otherwise the relative path.

【Default Configuration】 -The default file system is flash:, if the path name is not specified, it means the root path of the file system.

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】-

【Configuration Example]】1: Create a directory named newdir:

```
AC-FS#dir
Directory of flash:/
1-----rw-        336   Jan 03 2012 18:53:42  fstab
2-----rw-       4096   Jan 03 2012 12:32:09  rc.d
3-----rw-   10485760   Jan 03 2012 18:13:37  rpmdb
3 files, 0 directories
10,490,132 bytes total (13,192,656 bytes free) AC-
FS#mkdir newdir
Created dir flash:/newdir AC-
FS#dir
Directory of flash:/
1-----rw-        336   Jan 03 2012 18:53:42  fstab
2-----rw-       4096   Jan 03 2012 12:32:09  rc.d
3-----rw-   10485760   Jan 03 2012 18:13:37  rpmdb
4   drw-       4096     Jan   03   2012   18:13:37    newdir
3 files, 1 directories
10,494,228 bytes total (13,188,560 bytes free)
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

5.10more

Display the contents of a file.

more [/ascii | /binary] [filesystem:] file-url

【Parameter Description】

Parameter	Description
/ascii	Displays the file contents in the ASCII format.
/binary	Display the file contents in a 16-decimal / text format.
filesystem:	The url of the file system, followed with a colon, and possible file systems include: flash:, usb:, tmp:.
file-url	Path name, if starting with "/", indicates the absolute path, otherwise the relative path.

【Default Configuration】 By default, the original format of the file is displayed.

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】-

【Configuration Example]】1: Display the contents of the netconfig file in the root directory of the flash disk:

```
AC-FS#more flash:/netconfig#
# The network configuration file. This file is currently only used in
# conjunction with the TI-RPC code in the libtirpc library.
#
# Entries consist of:
#
#       <network_id> <semantics> <flags> <protofamily> <protoname> \
#               <device> <nametoaddr_libs>
#
# The <device> and <nametoaddr_libs> fields are always empty in this
# implementation.
#
udp        tpi_clts      v     inet     udp ----------
tcp        tpi_cots_ord  v     inet     tcp ----------
udp6       tpi_clts      v     inet6    udp ----------
tcp6       tpi_cots_ord  v     inet6    tcp ----------
rawip      tpi_raw       -     inet ----------
local      tpi_cots_ord  -     loopback ----------
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.11pwd

Displays the full path of the user's current working directory.

pwd

【Parameter Description】 -

【Default Configuration】 -

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】-

【Configuration Example】-

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

5.12 rename

Move an existing file or folder.

rename src-url dst-url

【Parameter Description】

Parameter	Description
src-url	Path and filename to be moved.
dst-url	The path and file name of the received file.

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】-

【Configuration Example]】1: Rename the fstab file in the root directory of the flash disk to new-fstab:

```
AC-FS#dir
Directory of flash:/
1------rw-         336    Jan 03 2012 18:53:42  fstab
2------rw-        4096    Jan 03 2012 12:32:09  rc.d

3------rw-    10485760    Jan 03 2012 18:13:37  rpmdb
3 files, 0 directories
10,490,192 bytes total (13,192,656 bytes free)
AC-FS#rename flash:/fstab flash:/new-fstab
Renamed file flash:/new-fstab
AC-FS#dir
Directory of flash:/
1------rw-         336    Jan 03 2012 18:53:42  new-fstab
2------rw-        4096    Jan 03 2012 12:32:09  rc.d
3------rw-    10485760    Jan 03 2012 18:13:37  rpmdb
3 files, 0 directories
10,490,192 bytes total (13,192,656 bytes free)
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

5.13rmdir

Delete an existing empty directory.

rmdir [filesystem:] directory

【Parameter Description】

Parameter	Description
filesystem:	URL of the file system, followed by a colon. Possible file systems include: Flash:, USB:, tmp:.
directory	-

【Default Configuration】 The default file system is flash:.

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】-

【Configuration Example]】1: The rmdir command deletes the existing empty directory of test:

AC-FS#mkdir newdir

```
AC-FS#dir
Directory of flash:/
1------rw-        336    Jan 03 2012 18:53:42  fstab
2------rw-       4096    Jan 03 2012 12:32:09  rc.d
3------rw-   10485760    Jan 03 2012 18:13:37  rpmdb
4   drw-       4096     Jan   03   2012   18:13:37    newdir
3 files, 1 directories
10,494,228 bytes total (13,188,560 bytes free) AC-
FS#rmdir newdir
removed dir flash:/newdir AC-
FS#dir
Directory of flash:/
1------rw-        336    Jan 03 2012 18:53:42  fstab
2------rw-       4096    Jan 03 2012 12:32:09  rc.d
3------rw-   10485760    Jan 03 2012 18:13:37  rpmdb
3 files, 0 directories
10,490,132 bytes total (13,192,656 bytes free)
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

5.14 show file systems

Displays information about the file system.

show file systems

【Parameter Description】-

【Command Mode】-

【Default Level】1

【Usage Guide】-

【Configuration Example]】1: Display information about all mounted file systems:

```
AC-FS#show file systems
  Size(KB)       Free(KB)     Type   Flags  Prefixes
        NA             NA      ram      rw  tmp:
        NA             NA  network      rw  tftp:
        NA             NA  network      rw  oob_tftp:
        NA             NA  xmodem      rw  xmodem:
      8192           2416     disk      rw  flash:
 167772160      147772160     disk      rw  sata0:
   1048576         548576     disk      rw  usb0:
    262144         152144     disk      rw  sd0:
```

Field Description:

Field	Description
Size(KB)	Space size of the file system, unit in KB.
Free(KB)	The remaining space of the file system, in KB.
Type	File system type.
Flags	The privileges of the file system are as follows: ro: read only wo: write only The rw:, Read and write
Prefixes	File system prefix.

【Prompt Information】-

【Platform Description】 -

5.15 show mount

Display system mount information.

show mount

【Parameter Description】-

【Command Mode】

【Default Level】1

【Usage Guide】-

【Configuration Example]】1: Display system mount information:

AC-FS#show mount

```
/dev/sda1 on / type ext4 (rw,errors=remount-ro,commit=0)
proc on /proc type proc (rw,noexec,nosuid,nodev)
sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
fusectl on /sys/fs/fuse/connections type fusectl (rw)
none on /sys/kernel/debug type debugfs (rw)
none on /sys/kernel/security type securityfs (rw)
udev on /dev type devtmpfs (rw,mode=0755)
devpts on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=0620)
tmpfs on /run type tmpfs (rw,noexec,nosuid,size=10%,mode=0755)
none on /run/lock type tmpfs (rw,noexec,nosuid,nodev,size=5242880)
none on /run/shm type tmpfs (rw,nosuid,nodev)
/dev/sda3 on /hao-share type ext3 (rw,commit=0)
binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,noexec,nosuid,nodev)
```

Field Description, take the first row as an example:

Field	Loaded properties
proc	Type of mount.
on	-
/proc	The destination address of the mount.
type	-
proc	The source address of the mount.
(rw,noexec,nosuid,nodev)	Mounted properties.

【Prompt Information】-

【Platform Description】 -

5.16tree

Displays the file tree of an existing directory.

tree [filesystem:] [directory]

【Parameter Description】

Parameter	Description
filesystem:	The url of the file system, followed with a colon, and possible file systems include: flash:, usb:, tmp:.
directory	Path name, if starting with "/", indicates the absolute path, otherwise the relative path.

【Default Configuration】 -The default file system is flash:.

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】-

【Configuration Example]】1: Display the file tree under flash:/echo:

```
AC-FS#tree flash:/echo
+-- client_module
+-- client_userspace
+-- echo_cli.c
+-- echo_client.c
+-- echo_client.h
+-- echo_client.o
+-- echo_cli.o
+-- echo_flag.h
+-- echo.h
+-- echo.ko
+-- echo_server.h
+-- exec_set_echo.h
+-- exec_show_echo.h
+-- Makefile
+-- module
¦   +-- echo.ko
¦   +-- echo.mod.c
¦   +-- echo.mod.o
¦   +-- echo_module.c
¦   +-- echo_module.o
¦   +-- echo.o
¦   +-- echo_server.c
¦   +-- echo_server.o
¦   +-- echo_sysfs.c
¦   +-- echo_sysfs.h
¦   +-- echo_sysfs.o
¦   +-- Makefile
¦   +-- modules.order
¦   +-- Module.symvers
¦   +-- msg_fd.c
¦   +-- msg_fd.o
+-- readme
+-- server_module
+-- server_userspace
+-- sys_rgos.ko
+-- user_space
```

```
    +-- echo_server.c
    +-- echo_server.o
    +-- Makefile
    +-- msg_fd.c
    +-- msg_fd.o 10,490,132 bytes total (13,192,656 bytes free)
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

5.17 verify

Calculate, display, and verify file md5 information

verify [/md5 md5-value] filesystem: [file-url]

【Parameter Description】

Parameter	Description
/md5	Calculate and displays the MD5 value of the file.
md5-value	The md5 value of the file will be compared to the calculated md5 value.
filesystem:	The url of the file system, followed with a colon, and possible file systems include: flash:, usb:, tmp:.
file-url	Path name, if starting with "/", indicates the absolute path, otherwise the relative path.

【Default Configuration】 The default file system is flash:.

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】-

【Configuration Example]】1: Calculate the md5 information of flash:/gcc:

```
AC-FS#verify flash:/gcc
8b072de7db7affd8b2ef824e7e4d716c
```

2: Calculate the md5 information of flash:/gcc and compare:

```
AC-FS#verify /md5 8b072de7db7affd8b2ef824e7e4d716c flash:/gcc
%SUCCESS verifying /mnt/flash/gcc = 8b072de7db7affd8b2ef824e7e4d716c AC-
FS#verify /md5 8b072de7db7affd8b2ef824e7e4d71 flash:/gcc
```

```
%Error verifying flash:/gcc
Computed signature = 8b072de7db7affd8b2ef824e7e4d716c
Submitted signature = 8b072de7db7affd8b2ef824e7e4d71
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

5.18 show disk

get usb info.

show disk usb/flash

【Parameter Description】

Parameter	Description
usb	Get the usb information.
flash	Get the flash information.

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】-

【Configuration Example]】1: View usb information:

```
AC-FS#show disk usb
Disk /dev/sdb: 8159 MB, 8159477760 bytes
252 heads, 62 sectors/track, 1020 cylinders
Units = cylinders of 15624 * 512 = 7999488 bytes
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6 SNMP

6.1 clear snmp locked-ip

To clear the source IP address table that is locked after SNMP consecutive authentication failures, execute the command clear snmp locked-ip. clear snmp locked-ip [ipv4 ipv4-address | ipv6 ipv6-address]

【Parameter Description】

Parameter	Description
ipv4 ipv4-address	Clears a specific source IPv6 address.
ipv6 ipv6-address	Clears a specific source IPv4 address.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 This command is used to manually clear the locked source IP address after SNMP continuous authentication fails. It can clear the entire source IP address table or a specific source IP address.

After the source IP address is cleared, SNMP access packets from this source IP address can re-try authentication.

【Configuration Example】 The following example clears the entire source IP address table that is locked after SNMP continuous authentication fails:

```
AC-FS# clear snmp locked-ip
```

【Prompt Information】-

【Platform Description】 -

6.2no snmp-server

Configure the shielding device SNMP agent function.

no snmp-server

【Parameter Description】-

【Default Configuration】 Enable SNMP agent function

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】The SNMP agent function service is enabled by default. In addition, when setting the SNMP agent parameters (such as NMS host address, authentication name and access authority, etc.), the SNMP agent service will also be automatically opened at the same time. Use this command to close all versions supported by the device. SNMP agent service.

This command must be turned on with the service switch command enable service snmp-agent at the same time, the SNMP agent service can take effect, but as long as one of them is turned off, the SNMP agent service will not take effect.

When this command is used, all SNMP agent service configurations will be blocked (that is, the configuration will not be displayed when viewing with the show running-config command, and the SNMP agent service can be restored by restarting the SNMP agent service), while the enable service snmp-agent command will not block the SNMP agent. configuration.

【Configuration Example】1: Shield SNMP agent service.

```
AC-FS(config)# no snmp-server
```

【Verification】Execute the no snmp-server command, and then execute the show running-config command to view the configuration. It can be found that all SNMP agent configuration commands are blocked except this command. The MIB cannot be accessed using NMS at this time.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.3 show snmp

Displays SNMP status information.

show snmp [mib | user | view | group | host | locked-ip | process-mib-time]

【Parameter Description】

Parameter	Description
mib	Displays the snmp mib information supported in the system.

user	Displays the snmp user information.
check	Displays the snmp view information.
group	Displays the snmp user group information.
host	Displays the display information for the user configuration.
locked-ip	Displays the source IP address information locked after the snmp continuous authentication failed.
process-mib-time	Displays the mib node with the longest processing time.

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Display is SNMP statistical information.

```
AC-FS# show snmp
Chassis: 60FF60
0 SNMP packets input
        0 Bad SNMP version errors
        0 Unknown community name
        0 Illegal operation for community name supplied
        0 Encoding errors
        0 Number of requested variables
        0 Number of altered variables
        0 Get-request PDUs
        0 Get-next PDUs
        0 Set-request PDUs
0 SNMP packets output
        0 Too big errors (Maximum packet size 1472)
        0 No such name errors
        0 Bad values errors
        0 General errors
        0 Response PDUs
        0 Trap PDUs
SNMP global trap: disabled
SNMP  logging:  disabled
SNMP agent: enabled
```

Field Description:

Field	Description

Chassis	Output message count: the total number of output messages.
SNMP packets input	Enter a message count: Total number of Set request messages.
Bad SNMP version errors	Enter a message count: the total number of Get-next request messages.
Unknown community name	Enter a message count: Total number of Get request messages.
Illegal operation for community name supplied	Enter a message count: the total number of MIB objects set.
Encoding errors	Enter a message count: the total number of MIB objects read.
Number of requested variables	Enter a message count: the total number of misencoded messages.
Number of altered variables	Enter a message count: the total number of messages using the group name.
Get-request PDUs	Enter a message count: the total number of messages accessed using an unknown group name.
Get-next PDUs	Enter a message count: the total number of messages with an incorrect version.
Set-request PDUs	Enter the message count: Enter the total number of messages.
SNMP packets output	System sequence code.
Too big errors (Maximum packet size 1472)	Output message count: the total number of extra-long (over 1,472 bytes) messages.
No such name errors	Output message count: Total number of messages returning No such name errors.
Bad values errors	Output message count: Total number of messages returning Bad values errors.
General errors	Output message count: Total number of messages returning General error errors.
Response PDUs	Output message count: the total number of messages returned normally.
Trap PDUs	Output message count: Total number of Trap messages issued.
SNMP global trap	Global Trap switch status.
SNMP logging	Global SNMP Log Switch status.
SNMP agent	Global SNMP Agent switch status.

【Prompt Information】-

【Platform Description】 -

6.4snmp trap link-status

Enable the interface to send Link Trap function.

snmp trap link-status

Disable the interface sending Link Trap function.

no snmp trap link-status

【Parameter Description】-

【Default Configuration】 By default, this function is enabled. If the Link state of the interface changes, SNMP will send a LinkTrap.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 For interfaces (Ethernet interface, Ap interface, SVI interface), when the function is turned on, if the interface changes Link state, SNMP will send Link Trap, otherwise it will not send it.

【Configuration Example】1: Disable the function of sending Link Trap on the interface.

```
AC-FS(config)# interface gigabitEthernet 1/1
AC-FS(config-if-GigabitEthernet 1/1)# no snmp trap link-status
```

2: Enable the interface to send Link Trap function.

```
AC-FS(config)# interface gigabitEthernet 1/1
AC-FS(config-if-GigabitEthernet 1/1)# snmp trap link-status
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.5snmp-server authentication attempt

This command is used to limit the number of consecutive SNMP authentication failures, and to specify the processing policy after consecutive authentication failures. The no form of this command clears the limit on the number of consecutive authentication failures

and related processing policies.

snmp-server authentication attempt times exceed { lock | lock-time minutes | unlock }

Clear the limit on the number of consecutive authentication failures and related processing policies.

no snmp-server authentication attempt times exceed { lock | lock-time minutes | unlock }

【Parameter Description】

Parameter	Description
times	The maximum number of SNMP authentication failures, range: 1~10.
exceed	The processing strategy adopted for the number of failures after SNMP authentication attempts exceeds the maximum limit.
lock	Indicates that the source IP address is permanently prohibited from being authenticated, and it is always blacklisted, which needs to be removed manually by the administrator.
lock-time minutes	Indicates that the source IP address is prohibited for a period of time before re-authentication; where minutes is the time for prohibiting the source IP address, range: 1 to 65535, unit: minutes.
unlock	Indicates that the user who fails the authentication will not be restricted and is allowed to continue to log in.

【Default Configuration】 By default, the SNMP attack protection detection function is disabled.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 After the SNMP authentication fails, the system will add it to the blacklist managed by the SNMP source IP address. When the number of authentication failures exceeds the limit, the system will restrict the subsequent access authentication behaviors according to the processing measures set by the device:

1. For the source IP address that has been permanently banned from authentication, the source IP address can re-access authentication only after the administrator manually releases it;

2. For the source IP address that has been banned from authentication for a period of time, the source IP address can be re-authenticated only after the set ban time expires or the administrator manually cancels it;

For unrestricted source IP addresses, as long as the user re-authenticates with the correct community (y for SNMPv1 and SNMPv2c) or username (for SNMPv3), re-authentication is successful.

【Configuration Example]】1: The following example sets the number of consecutive SNMP authentication failures to 4, and locks for 30 minutes after 4 consecutive authentication failures:

```
AC-FS(config)# snmp-server authentication attempt 4 exceed lock-time 30
```

【Verification】After the SNMP attack protection detection function is enabled, use the wrong community name or wrong user name for access authentication. After continuous authentication fails, the source IP address will be locked. When the authentication is accessed again, there will be a log that the IP has been locked. Use show snmp locked-ip to see that the IP address is in the lock list.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.6snmp-server cache enable

Configure the global SNMP MIB cache function.

snmp-server cache enable

Disable the SNMP MIB cache function.

no snmp-server cache enable

【Parameter Description】-

【Default Configuration】 By default, this function is disabled.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】The following example enables the SNMP MIB cache function:

```
AC-FS(config)# snmp-server cache enable
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.7snmp-server cache oid

Configure the specified OID node to enable the cache function, and the specified OID node cache update time.

snmp-server cache oid oid-string [update-timer seconds]

Turn off the cache function of the specified OID node, or restore the cache update time of the specified OID node.

no snmp-server cache oid oid-string [update-timer]

【Parameter Description】

Parameter	Description
oid-string	The MIB Node OID.
seconds	SNMP MIB Global Cache update time in seconds, ranging from 60 to 3600.

【Default Configuration】 MIB node cache function is not enabled.

The default cache update time is the globally configured cache update time.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】If the cache update time is not configured, the globally configured cache update time will be used as the cache update time of the OID node.

Use the no snmp-server cache oid oid-string update-timer command to delete the cache update time configuration of the specified OID node, and use the globally configured cache update time as the cache update time of the OID node.

【Configuration Example】The following example configures the SNMP MIB node to enable the cache function:

```
AC-FS(config)# snmp-server cache oid 1.3.6.1.4.1.4881.1.1.10.2.56.2.1.1.1
```

The following example configures the SNMP MIB node cache update time to be 600 seconds:

```
AC-FS(config)# snmp-server cache oid 1.3.6.1.4.1.4881.1.1.10.2.56.2.1.1.1 update-timer 600
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.8 snmp-server cache update-timer

Configure the SNMP MIB global cache update time.

snmp-server cache update-timer seconds

Restore the SNMP MIB cache update time to the default value.

no snmp-server cache update-timer

【Parameter Description】

Parameter	Description
seconds	SNMP MIB Global Cache update time in seconds, ranging from 60 to 3600.

【Default Configuration】 The default cache update time is 300 seconds.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】The following example configures the update time of the SNMP MIB cache function to be 600 seconds:

```
AC-FS(config)# snmp-server cache update-timer 600
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.9snmp-server chassis-id

Configure the system serial code.

snmp-server chassis-id text

Restore default values.

no snmp-server chassis-id

【Parameter Description】

Parameter	Description
text	The text of the system serial number, which can be a number or a character.

【Default Configuration】 The default value of the serial number is 60FF60.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 The serial number of the SNMP system generally uses the serial number of the machine to identify the device. The system serial number can be viewed with the show snmp command.

【Configuration Example】1: The serial number of the system configured with SNMP is 123456.

```
AC-FS(config)# snmp-server chassis-id 123456
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.10snmp-server community

Configure the authentication name and access rights.

snmp-server community [0 | 7] string [view view-name] [[ro | rw] [host ipaddr]] [ipv6 ipv6-aclname] [aclnum | aclname]

Delete the authentication name.

no snmp-server community [0 | 7] string

【Parameter Description】

Parameter	Description
0	The group string indicating the input is a plaintext string
7	The group string representing the input is a ciphertext string
string	The group string, equivalent to the communication password between the NMS and the SNMP agent.
Check-name	Specifies the name of the view for view-based management.
ro	Variables that specify that NMS are read-only to MIB and cannot be modified.
rw	The NMS is readable and writable for the variables of the MIB.
aclnum	The access list serial number (1-199) is associated with the specified access list and specifies the ipv4NMS address range that can access the MIB.
aclname	The access list name is associated with the specified access list, and specifies the ipv4 NMS address range that can access the MIB.
ipv6-aclname	The name of the ipv6 access list, which is associated with the specified access list, and specifies the ipv6 NMS address range that can access the MIB.
ipaddr	Associate the NMS address to specify the NMS address that access the MIB.
ipv6-aclname	The name of the ipv6 access list, which is associated with the specified access list, and specifies the ipv6 NMS address range that can access the MIB.
ipaddr	Associate the NMS address to specify the NMS address that access the MIB.

【Default Configuration】 All communities are read-only by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command is the first important command to enable the SNMP agent function of the device. It specifies the

attributes of the community, the range of NMS that is allowed to access the MIB, and so on. To disable the SNMP agent function, execute the no snmp-server command.

【Configuration Example]】1: Configure to allow the NMS to use the public SNMP community access character to access the MIB, and the permission is read-only.

```
AC-FS(config)# snmp-server community public ro
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.11snmp-server contact

Configure the contact information of the system.

snmp-server contact text

Delete the specified contact information.

no snmp-server contact

【Parameter Description】

Parameter	Description
text	String of the Description system contact information.

【Default Configuration】 The system contact information is empty.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: The system contact information for configuring SNMP is i-net800@i-net.com.cn.

```
AC-FS(config)# snmp-server contact i-net800@i-net.com.cn
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.12 snmp-server enable secret-dictionary-check

Configure password dictionary checking for community and user.

snmp-server enable secret-dictionary-check

Revoke password dictionary checks for community and user.

no snmp-server enable secret-dictionary-check

【Parameter Description】-

【Default Configuration】 By default, the password dictionary check for community and user is not performed.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command must be used together with the global configuration command password policy.

【Configuration Example】1: The length of the configuration password is not less than 6 characters.

```
AC-FS(config)# password  policy  min-size  6 AC-FS(config)#
snmp-server enable secret-dictionary-check AC-
FS(config)#snmp-server community abc12
% The community(abc12) is a weak community!
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.13 snmp-server enable traps

Configure the Agent to actively send Trap messages to the NMS.

snmp-server enable traps [notification-type]

Disable SNMP from actively sending Trap messages to NMS.

no snmp-server enable traps

【Parameter Description】

Parameter	Description
notification-type	Trap types that are actively sent, there are the following types: snmp: start TRAP notification of SNMP events; bridge: start TRAP notification of BRIDGE event; mac-notification: start TRAP notification of MAC events; ospf: start TRAP notification of OSPF events; urpf: Initiate TRAP notification of URPF events; vrrp: start TRAP notification of VRRP events; web-auth: Enable TRAP notification of web authentication events.

【Default Configuration】 By default, SNMP is prohibited from actively sending Trap messages to NMS.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command must be used together with the global configuration command snmp-server host to send Trap messages. If no Trap type is specified, all Trap types are included.

【Configuration Example]】 1: Configure to actively send SNMP event trap messages.

```
AC-FS(config)# snmp-server enable traps snmp
AC-FS(config)# snmp-server host 192.168.12.219 public snmp
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.14 snmp-server flow-control

Configure SNMP flow control.

snmp-server flow-control pps [count]

Restore the default value of SNMP flow control.

no snmp-server flow-control pps

【Parameter Description】

Parameter	Description
count	Number of SNMP request messages processed per second, range <50-65535>.

【Default Configuration】 Default Configuration count is 150.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure to process 200 SNMP request packets per second.

```
AC-FS(config)# snmp-server flow-control pps 200
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.15snmp-server group

Configure SNMP user groups.

snmp-server group groupname { v1 | v2c | v3 { auth | noauth | priv } } [read readview] [write writeview] [access { ipv6 ipv6-aclname | aclnum | aclname }]

Delete user group.

no snmp-server group groupname { v1 | v2c | v3 {auth | noauth | priv} }

【Parameter Description】

Parameter	Description
v1 | v2c |v3	Indicates the SNMP version.
auth	The messages transmitted by users of this group need to be authenticated but the data does not need to be kept secret, only valid for v3.
noauth	The messages transmitted by this group of users do not require authentication data or confidentiality, and are only valid for v3.
priv	The messages transmitted by this group of users need to be verified and the data transmitted at the same time needs to be kept secret, which is only valid for v3.
readCheck	Associate a read-only view.
writeCheck	Associate a read-write view.
aclnum	The serial number of the access list is associated with the specified access list and specifies the ipv4 NMS address range that can access the MIB.
aclname	The access list name is associated with the specified access list, and specifies the ipv4 NMS address range that can access the MIB.
ipv6-aclname	The name of the ipv6 access list, which is associated with the specified access list, and specifies the ipv6 NMS address range that can access the MIB.

【Default Configuration】 There is no user group configured by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure a user group mib2user.

```
AC-FS(config)# snmp-server group mib2user v3 priv read mib2
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.16snmp-server host

Configure the NMS host address where the Agent actively sends messages.

snmp-server host { host-addr | ipv6 ipv6-addr } [traps | informs] [version { 1 | 2c | 3 { auth | noauth | priv }] community-string [udp-port port-num] [notification-type]

Deletes the specified SNMP host address.

no snmp-server host { host-addr | ipv6 ipv6-addr } [traps | informs] [version { 1 | 2c | 3 { auth | noauth | priv }] community-string [udp-port port-num]

【Parameter Description】

Parameter	Description
host-addr	SNMP host address.
ipv6-addr	SNMP Host Address (ipv6).
traps | informs	Configure the host to send a trap message or a inform message.
version	Select the snmp version, V1, V2C, and V3.
auth | noauth | priv	Configure the security level of the V3 user.
community-string	Group string or username (V3 version).
port-num	Configure the snmp host port.
notification-type	Type of Trap proactively sent, for example, snmp. If the Trap type is not specified, all Trap types are included.

【Default Configuration】 By default, there is no SNMP host.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command is used together with the global configuration command snmp-server enable traps to actively send trap messages to the NMS.

Multiple different SNMP hosts can be configured to receive Trap messages. One host can use different combinations of Trap types and different ports. For the same host, the last configuration will be merged with the previous configuration. Trap messages, you can configure different Trap types separately, and eventually these configurations will be merged together.

【Configuration Example】1: Specify an SNMP host to receive SNMP event Trap.

```
AC-FS(config)# snmp-server host 192.168.12.219 public snmp
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.17 snmp-server inform

Configure the number of attempts to send inform and the timeout sending time.

snmp-server inform [retries retry-num | timeout time]

Recover the number of retransmission attempts and timeout sending time of the inform message.

no snmp-server inform

【Parameter Description】

Parameter	Description
retry-num	Rehair attempts in Inform message, range <0-255>.
time	The Inform message was timed out to send the time, the range is <0-21474836>.

【Default Configuration】 Default Configuration retry-num is 3, time is 15s.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the number of attempts to retransmit the inform message to 5.

```
AC-FS(config)# snmp-server inform retries 5
```

2: Configure the inform message timeout sending time to 20s.

```
AC-FS(config)# snmp-server inform timeout 20
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.18snmp-server location

Configure the system location.

snmp-server location text

Delete system location.

no snmp-server location

【Parameter Description】

Parameter	Description
text	String of the Description system information.

【Default Configuration】 System information is empty

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Configure the system location.

```
AC-FS(config)# snmp-server location start-technology-city 4F of A Building
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.19 snmp-server logging

The SNMP log function will record the GET, GET-NEXT and SET operations of the NMS to the SNMP Agent

snmp-server logging { get-operation | set-operation }

Close open switch

no snmp-server logging { get-operation | set-operation }

【Parameter Description】

Parameter	Description
get-operation	Record the switches operated by the GET and GET-NEXT.
set-operation	Record the switch operating by the SET.

【Default Configuration】 By default, the SNMP log function is disabled.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to record the GET, GET-NEXT, and SET operations of the NMS to the SNMP Agent. When performing GET and GET-NEXT operations, the Agent will record the IP address of the NMS user, the operation type, and the node OID of the operation. When the SET operation is performed, the Agent will record the IP address of the NMS user, the operation type, the node OID of the operation and the set value.

A large number of log records will affect the performance of the device. Under normal circumstances, it is recommended to disable the SNMP log function.

【Configuration Example]】1: Turn on the record switch of get and set operations.

```
AC-FS(config)#snmp-server logging get-operation
AC-FS(config)#snmp-server logging set-operation
```

Perform GET, GET-NEXT and SET operations on the sysname node (.1.3.6.1.2.1.1.5.0) through NMS, the console will print the following log information.

```
AC-FS#*Feb 7 15:31:16: %SNMP-6-GET_OPER: NMS source-ip(13.12.11.7) operation(GET)
object(id=1.3.6.1.2.1.1.5.0)

AC-FS#*Feb 7 15:32:16:%SNMP-6-GETN_OPER: NMS source-ip(13.12.11.7) operation(GET-NEXT)
object(id=1.3.6.1.2.1.1.5.0)

AC-FS#*Feb 7 15:33:23: %SNMP-6-SET_OPER: NMS source-ip(13.12.11.7) operation(SET)
object(id=1.3.6.1.2.1.1.5.0, value=AC-FS)
```

2: Turn off the get or set switch.

```
AC-FS(config)#no snmp-server logging get-operation
AC-FS(config)#no snmp-server logging set-operation
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.20snmp-server net-id

Configure device NE coding information.

snmp-server net-id text

Delete the device NE coding information.

no snmp-server net-id

【Parameter Description】

Parameter	Description
text	Set the device NE code text, text is a string with a length of 1~255, case-sensitive, and can contain spaces.

【Default Configuration】 The device NE code information is empty

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the device NE coding information.

```
AC-FS(config)# snmp-server net-id FZ_CDMA_MSC1
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.21snmp-server packetsize

Configure the maximum data packet length of the SNMP agent.

snmp-server packetsize byte-count

Restore default values.

no snmp-server packetsize

【Parameter Description】

Parameter	Description
byte-count	Package size, from 484 bytes to 17,876 bytes.

【Default Configuration】 1472 bytes.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Configure the maximum packet size of SNMP as 1492.

```
AC-FS(config)# snmp-server packetsize 1492
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.22snmp-server queue-length

Configure the queue length of trap messages.

snmp-server queue-length length

Restore default values.

no snmp-server queue-length

【Parameter Description】

Parameter	Description
length	Queue length, size from 1 to 1000. The default value is 100.

【Default Configuration】 100

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】Control the message sending speed by adjusting the size of the message queue. The maximum message sending speed is 4 per second.

【Configuration Example]】1: Configure the Trap message queue length to be 4.

```
AC-FS(config)# snmp-server queue-length 4
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.23 snmp-server system-shutdown

Enable SNMP system restart notification function.

snmp-server system-shutdown

Disable the SNMP system restart notification function.

no snmp-server system-shutdown

【Parameter Description】-

【Default Configuration】 Disable the SNMP system restart notification function.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】Enable the SNMP system restart notification function, RGOS will send a trap message to the NMS to notify the system to restart before the device reload/reboot.

【Configuration Example】1: Enable SNMP system restart notification function.

```
AC-FS(config)# snmp-server system-shutdown
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.24 snmp-server trap-format private

Configure SNMP Trap messages to carry private Fields.

snmp-server trap-format private

Restore Default Configuration.

no snmp-server trap-format private

【Parameter Description】-

【Default Configuration】 Does not carry private Field.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】Use this command to configure the private format Field to be sent in the Trap message. The included Field currently supports the alarm occurrence time. For the specific data type and data range of each Field, please refer to AC-FS-TRAP-FORMAT-MIB.mib File description.

This configuration does not take effect when trap messages are sent using SNMP v1.

【Configuration Example]】1: Specify the Trap message to carry a private Field.

```
AC-FS(config)# snmp-server trap-format private
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.25 snmp-server trap-source

Specifies the source address for sending trap messages.

snmp-server trap-source interface

Restore Default Configuration.

no snmp-server trap-source

【Parameter Description】

Parameter	Description
interface	Interface used as the SNMP source address.

【Default Configuration】 The IP address of the interface from which SNMP packets are sent out is used as the source address.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】By default, the IP address of the interface is used as the source address from which interface the SNMP packets go out. For the convenience of management and identification, you can use this command to use a fixed local IP address as the source address of SNMP.

【Configuration Example】1: Specify the IP address of Ethernet port 0/1 as the source address for sending Trap messages.

```
AC-FS(config)# snmp-server trap-source fastethernet 0/1
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.26 snmp-server trap-timeout

Configure the timeout period for resending trap messages.

snmp-server trap-timeout seconds

Restore Default Configuration.

no snmp-server trap-timeout

【Parameter Description】

Parameter	Description
seconds	Timeout time, in seconds, take the value range: 11,000.

【Default Configuration】 30 seconds

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure the timeout period for retransmission of trap messages to be 60 seconds.

```
AC-FS(config)# snmp-server trap-timeout 60
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.27 snmp-server udp-port

Specifies the protocol port number for receiving SNMP packets.

snmp-server udp-port port-num

Restore Default Configuration.

no snmp-server udp-port

【Parameter Description】

Parameter	Description
port-num	Specifies the protocol port number to receives the SNMP message.

【Default Configuration】 By default, the 161 protocol port is used to receive SNMP packets.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Specify the 15000 protocol port to receive SNMP packets.

```
AC-FS(config)# snmp-server udp-port 15000
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.28 snmp-server user

Configure SNMP users.

snmp-server user username groupname {v1 | v2c | v3 [encrypted] [auth {md5 | sha} auth-password] [priv des56 priv-password]} [access {ipv6 ipv6-aclname | aclnum | aclname}]

Delete SNMP users.

no snmp-server user username groupname {v1 | v2c | v3 }

【Parameter Description】

Parameter	Description
username	user name.
groupname	The group name corresponding to the user
v1 | v2c | v3	Indicates the SNMP version. Only v3 supports the later security Parameter.
encrypted	The specified password input method is cipher text input. Otherwise, enter it in clear text. If you choose to enter in cipher text, you need to enter the key represented by consecutive hexadecimal numeric characters. Note that the authentication key length using MD5 is 16 bytes, while the SHA authentication protocol key length is 20 bytes. A byte is represented by two characters. The encrypted representation of the key is only valid for this engine.
auth	Specifies whether to use the validation.
md5	Specifies the use of the MD5 authentication protocol. The sha specifies the use of the SHA authentication protocol.
auth-password	Configure the password string used by the authentication protocol (32 characters or less). The system converts these passwords into corresponding authentication keys.
priv	Specifies whether secrecy is used. The des56 indicates that the 56-bit DES encryption protocol is used.
priv-password	Password string for encryption (up to 32 characters). The system converts this password into the corresponding encryption key.
aclnum	The serial number of the access list is associated with the specified access list and specifies the ipv4 NMS address range that can access the MIB.
aclname	The access list name is associated with the specified access list, and specifies the ipv4 NMS address range that can access the MIB.
Ipv6-aclname	The name of the ipv6 access list, which is associated with the specified access list, and specifies the ipv6 NMS address range that can access the MIB.

【Default Configuration】 There is no user configured by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure an SNMPv3 user, use MD5 authentication, and use DES encryption.

```
AC-FS(config)# snmp-server user user-2 mib2user v3 auth md5 authpassstr priv des56 despassstr
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.29 snmp-server view

Configure SNMP views.

snmp-server view view-name oid-tree {include | exclude}

Delete the SNMP view.

no snmp-server view view-name [oid-tree]

【Parameter Description】

Parameter	Description
Check-name	View name.
oid-tree	The MIB object, is a MIB subtree.
include	Indications are that the MIB object subtree is included in the view.
exclude	Indication that the MIB object subtree was excluded from the view.

【Default Configuration】 Default Configuration is a default view that allows access to all MIB objects.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example]】1: Configure a view, including all MIB-2 subtrees (oid is 1.3.6.1).

```
AC-FS(config)# snmp-server view mib2 1.3.6.1 include
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

7 HTTP

7.1 enable service web-server

Turn on the HTTP service function.

enable service web-server [http | https | all]

Turn off the HTTP service function.

{ no | default } enable service web-server [http | https | all]

【Parameter Description】

Parameter	Description
http | https | all	Open the appropriate service.For http to open HTTP service, https to open HTTPS service, all Open both the HTTP and HTTPS services for you.The default is to open both the HTTP and HTTPS services.

【Default Configuration】 The HTTP service and HTTPS service functions are disabled.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 If the command is executed without any keyword or followed by all, it means that both HTTP service and HTTPS service are opened; if it is followed by http keyword, it means that only HTTP service is opened; if it is followed by https keyword, it means that only HTTPS service is opened .

Use no enable service web-server or default enable service web-server to disable the corresponding HTTP service. If the no command or the default command is not followed by any keyword, it means that the HTTP service and the HTTPS service are closed at the same time.

【Configuration Example]】1: Enable HTTP and HTTPS service functions at the same time.

```
AC-FS(config)# enable service web-server
```

【Verification】1: Use the show service command to view the current service status of the system.

2: Use the show web-server status command to view the web server status.

【Prompt Information】 1: When opening the HTTP service, if the port is 80 and the opening fails, it will prompt.

```
%notice:Failed to open tcp listen, port=[80].
```

【Common Mistake】 1. If the port is occupied by other modules, it may fail to open the Web service.

【Platform Description】 -

7.2http check-version

Detect updatable file information in the HTTP server.

http check-version

【Parameter Description】-

【Default Configuration】 Detect the version information of files that can be upgraded in the HTTP server.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 The user can use this command to detect the file type that needs to be upgraded, and the detected file is the file that is newer than the local server.

【Configuration Example]】1: Detect the HTTP upgrade version.

```
AC-FS# http check-version
Business modules need to be updated: character-db, route-db
app name:web
    app-name           version          filename
_______________ ____________________ _______________________

character-db    2014.02.09.14.02.09  app_sub_1.exe  character-db
2014.02.09.14.02.09        app_file_list.txt        character-db
2014.02.09.14.02.09          app_sub_3.exe          character-db
2014.02.09.14.02.09            app_sub_2.exe            route-db
2013.12.01.00        route-choose.db
```

【Verification】-

【Prompt Information】 1: If no business module is currently registered in the upgrade module.

```
%notice: No bussiness modules registration.
```

2: If the connection to the server cannot be established or the communication with the server fails, the following Prompt Information is given.

```
%notice: Communicate with the server failed.
```

3: If the device application memory is insufficient.

```
%warning: Out of memory, application memory failure.
```

4: If the format of the server response message is incorrect.

```
%notice: The server response message format is wrong.
```

5: If the business module is being upgraded or there is no registered version number.

```
%notice: Suspend, some business modules are upgrading or haven't registered release.
```

6: If all business module versions are up to date.

```
%notice: All bussiness modules are the latest versions.
```

【Common Mistake】 1. When this command is executed, it prompts that the communication with the server fails. It may be that the network is blocked or the DNS service is not enabled.

【Platform Description】 -

7.3 http update

Manually upgrade files.

http update { all | string }

【Parameter Description】

Parameter	Description
all	Upgrade all of the business modules.
string	Business module names that need to be upgraded, you can enter multiple, and the names are divided by spaces.

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 The user can manually upgrade the specified service module through this command.

【Configuration Example]】1: Manually download and upgrade the latest route-db and url-db in the remote server.

```
AC-FS# http update route-db
Downloading updated files, please wait...
Press Ctrl+C to quit
route-db: download and notify successfully.
```

【Verification】1: Use the http check-version command to check the file information that can be upgraded in the HTTP server.

【Prompt Information】1: If no business module is currently registered in the upgrade module.

%notice: No bussiness modules registration.

2: If the specified business module is not registered, the following Prompt Information is given.

%notice: The bussiness modules haven't registered.

3: If the current upgrade module is being upgraded, the following Prompt Information is given.

%notice: There are business modules in the upgrading, please wait for a moment.

4: If the connection to the server cannot be established or the communication with the server fails, the following Prompt Information is given.

%notice: Communicate with the server failed.

5: If the device application memory is insufficient.

%warning: Out of memory, application memory failure.

6: If the format of the server response message is incorrect.

%notice: The server response message format is wrong.

7: If the business module is being upgraded or there is no registered version number.

%notice: Suspend, some business modules are upgrading or haven't registered release.

8: If all business module versions are up to date.

%notice: All bussiness modules are the latest versions.

【Common Mistake】 1. When this command is executed, it prompts that the communication with the server fails. It may be that the network is blocked or the DNS service is not enabled.

【Platform Description】 -

7.4 http update mode

Configure the HTTP upgrade mode to manual upgrade mode.

http update mode manual

Revert to automatic upgrade mode.

no http update mode

【Parameter Description】

Parameter	Description
manual	Manual upgrade mode.

【Default Configuration】 The default is automatic upgrade mode.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Use this command to configure HTTP upgrade mode.

Configure this command, HTTP is the manual upgrade mode.

Execute the no form of this command. HTTP is the automatic upgrade mode. When the automatic upgrade time is up, the file information that can be upgraded by the server will be detected by default, and the upgrade will be downloaded automatically.

【Configuration Example]】1: Set the HTTP upgrade mode to automatic detection mode.

```
AC-FS(config)# http update mode manual
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

7.5 http update server

Configure the server address and port number for HTTP upgrade.

http update server { host-name | ip-address } [port port-number]

Delete the configured HTTP upgrade server and restore the default value.

no http update server

【Parameter Description】

Parameter	Description
host-name	Server domain name.
ip-address	Server address.
port port-number	Server-side slogan, the value range is 1-65535. The default rate is 80.

【Default Configuration】 The default server address is 0.0.0.0 and the port number is 80.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Use this command to configure the server address and port number for HTTP upgrade.

During HTTP upgrade, connect to the server address configured by this command first. If the connection fails, it will try to connect to the locally recorded server address one by one. If all servers cannot be connected, the upgrade cannot be performed.

The system will record the address information of one or more upgrade servers, and these addresses are not allowed to be modified.

The server address is not configured because the possible upgrade server address is recorded in the local upgrade record file.
By default, open the DNS feature and configure the DNS server address.
IPV6 is not supported at the server address.

【Configuration Example]】1: Configure the address of the HTTP upgrade server as 10.83.132.1 and the port number as 90.

```
AC-FS(config)# http update server 10.83.132.1 port 90
```

【Verification】-

【Prompt Information】

【Common Mistake】-

【Platform Description】 -

7.6 http update time

Configure HTTP auto-detection time.

http update time daily hh:mm

Delete the configured HTTP auto-detection time and restore the Default Configuration.

no http update time

【Parameter Description】

Parameter	Description
hh:mm	The specific upgrade time, the format is hours (24 hours): minutes.

【Default Configuration】 The default automatic detection time is a random time between 00:00 – 23:59.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】This command is used to configure the HTTP automatic detection time. The device will automatically connect to the Web server (rgos.AC-FS.com.cn) at the specified time every day to detect whether there is any upgradeable file information. The obtained file information can be viewed through the web interface.

When the no form of this command is executed, the device detection time is random.

【Configuration Example]】1: Configure the HTTP automatic detection time to 23:40.

```
AC-FS(config)# http update time daily 23:40
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

7.7ip http port

Set the port for the HTTP service.

ip http port port-number

Restore the default port.

no ip http port

【Parameter Description】

Parameter	Description
port-number	Set up the HTTP service port with a value range of 80 and 1025-65535.

【Default Configuration】 The default port number is 80.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Use this command to set the port of HTTP service.

【Configuration Example]】1: Set the service port of HTTP to 8080.

```
AC-FS(config)# ip http port 8080
```

【Verification】Use the show web-service command to view the status of the web server.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

7.8ip http secure-port

Set the port for the HTTPS service.

ip http secure-port port-number

Restore the default port.

no ip http secure-port

【Parameter Description】

Parameter	Description
port-number	Set up the HTTPS service port for 4430 and 1025-65535.

【Default Configuration】 The default port number is 4430.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Use this command to set the port of HTTPS service.

【Configuration Example]】1: Set the service port of HTTPS to 4443.

```
AC-FS(config)# ip http secure-port 4443
```

【Verification】Use the show web-service command to view the status of the web server.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

7.9show web-server https certificate information

View HTTPS service certificate information.

show web-server https certificate information

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to view HTTPS service certificate information.

【Configuration Example]】 1: View HTTPS service certificate information.

```
AC-FS# show web-server https certificate information
Source: Default
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=Self-Signed-CA472E87
        Validity
            Not Before: Feb 20 07:26:51 2019 GMT
            Not After : Feb 17 07:26:51 2029 GMT
        Subject: CN=Self-Signed-CA472E87
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
```

```
            Modulus:
                00:ec:39:13:5a:09:da:97:d1:83:8f:a7:77:cf:b4:
                88:96:a0:85:23:68:4d:5a:c6:d3:4b:d9:c0:d6:1b:
                f4:42:29:ce:33:2e:2f:79:5e:cc:bb:bd:5f:63:5b:
                41:f3:9f:fb:82:c7:ca:8a:21:a9:c2:fb:36:db:62:
                08:3c:05:b8:a2:47:07:1a:20:99:80:24:63:a4:08:
                66:22:86:b6:aa:46:43:8a:91:7d:99:f3:8a:7c:58:
                ac:1f:ef:6c:4c:d1:d6:bf:ef:a1:77:64:4b:53:16:
                29:2f:1c:e8:ec:d6:6b:b6:34:64:32:00:1f:09:30:
                69:8d:2e:85:d5:6a:db:45:cb:b8:fd:38:ba:bd:68:
                1d:de:38:65:ef:3f:c6:90:bf:ca:1a:9e:df:c3:75:
                5f:20:bd:61:b4:bd:43:6b:77:ef:25:c6:43:0a:0f:
                dc:5a:0e:28:53:37:14:77:8b:bd:ea:14:54:c5:e1:
                45:27:c9:14:63:37:67:bc:0f:09:15:1f:73:ae:bb:
                46:b1:ad:cd:23:89:fd:2c:0c:9f:a3:34:62:f0:14:
                0d:c8:92:09:68:df:8f:69:fb:1c:49:91:d8:1c:f7:
                ee:67:a3:25:c5:9a:e2:f6:1c:a8:8c:af:7e:08:29:
                44:32:b1:d8:a9:86:04:a2:80:65:24:47:56:f4:fd:
                e4:19
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
Signature Algorithm: sha256WithRSAEncryption
     16:b8:e2:1e:45:13:56:9c:48:ef:ec:40:fb:9a:e3:4c:da:e4:
     95:c4:3b:92:10:9a:27:a0:da:ab:45:86:4c:39:fd:73:0c:e8:
     98:8b:0e:a4:28:72:66:0a:74:cc:9c:91:71:2f:94:dd:4b:4b:
     a2:54:e5:8f:47:82:bd:82:4d:70:93:6e:af:72:ce:cf:db:e2:
     36:b1:64:1a:1f:5e:c1:d9:57:12:15:5f:81:d3:ab:40:66:2a:
     3d:ab:d4:fb:24:a6:dd:1f:82:a2:33:9d:3d:da:a7:75:fa:0d:
     e6:be:1f:3b:a9:7f:d0:94:67:bf:e7:8b:19:32:5c:ea:0f:ae:
     3e:1e:41:55:06:c9:cb:42:b9:45:de:0e:d9:48:a5:75:90:5b:
     d7:89:ff:60:f2:31:ed:d7:52:0a:3d:91:87:c3:9a:85:76:8a:
     44:6f:c5:4e:9b:65:f6:78:cf:ee:7b:28:f5:10:c8:d1:39:3f:
     13:a7:96:f1:4b:11:5f:34:96:8f:13:b1:b6:de:9c:23:9e:f6:
     9d:b8:a3:f7:03:07:76:ce:bd:f6:76:1d:fc:5d:83:1e:8e:74:
     fb:78:b6:4a:ad:73:ce:e7:71:72:7d:0a:1e:49:5d:9e:65:30:
     aa:6f:b4:2f:9d:c3:e5:e6:38:de:0b:26:20:69:98:e4:6d:99:
     d2:15:ec:bd
```

Field Description:

Field	Instruction
Source	Certificate source, which may have the following values: Default: Use the default self-signed certificate. Installed: Use the certificate installed by the user.
Certificate	Certificate information.

【Prompt Information】-

【Platform Description】 -

7.10 show web-service

View web service configuration information and status.

show web-service

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to view the configuration information and status of the Web service.

【Configuration Example]】1: View the configuration information and status of the Web service.

```
AC-FS#show web-service
webservice  :
  http      : enable
            : port(9999)
  https     : enable
            : port(4430)
```

Field Description:

Field	Instruction
http enable(disable)	Status of the HTTP service.
http port	Ports of the HTTP service.
https enable(disable)	Status of the HTTP service.

https port	Ports of the HTTP service.

【Prompt Information】-

【Platform Description】 -

7.11 webmaster level

Set the Web login authentication user name and password.

webmaster level privilege-level username name password { password | [0 | 7] encrypted-password }

Restore Default Configuration.

no webmaster level privilege-level [username name]

【Parameter Description】

Parameter	Description
privilege-level	User-binding permission level.
name	user name.
password	user password.
0 | 7	The encryption type of the password, 0 no encryption, 7 simple encryption. The default is 0.
encrypted-password	Password text

【Default Configuration】 The default user binding permission level is 0, and the plaintext password is admin.

The default user binding permission level is 2, the user name is guest, and the plaintext password is guest.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 When using the Web Server, login authentication is required to enter the Web page. Use this command to set the username and password for Web login authentication.

Execute no webmaster level privilege-level to delete all user names and passwords of the specified privilege level. Execute no webmaster level privilege-level username name to delete the specified username and password.

User name and password have three permission levels; each permission level can be configured with up to 10 user names and passwords.

By default, two accounts, admin and guest accounts, two accounts cannot be deleted, only the password can be modified. By default, the guest account corresponds to level 2 permission, and only has the permission to view the home page of the system at the web end. The administrator account is admin corresponding to level 0 permission, with all functions on the web end, and can edit other management accounts and authorize the page to access. The newly added account corresponds to level 1 permission.

【Configuration Example]】 Configure the user binding permission level of Web login authentication to 0, the user name to be AC-FS, and the password to be admin.

```
AC-FS(config)# webmaster level 0 username AC-FS password admin
```

【Verification】 -

【Prompt Information】 1: If the admin or guest authentication information of the default configuration is deleted, the following prompt will be given.

```
notice: Cannot cancel the default user configure!
```

2: If there are more than 10 user names configured for each permission level, the following prompt will be given.

```
%notice: configure webmaster level %d server reached max 10, add failed.
```

3: If the configured username reaches or exceeds 32 characters, the following prompt will be given.

```
%notice: Username too long. Please enter less than 32 characters.
```

【Common Mistake】 -

【Platform Description】 -

7.12 web-server https certificate

Install the HTTPS service certificate

web-server https certificate { pem cert-filename private-key key-filename } | { pfx cert-filename } [password password-text]

Restore Default Configuration.

no web-server https certificate

【Parameter Description】

Parameter	Description
pem	Import the certificate files and the private key files in pem format.

pfx	Import a certificate file in pfx format that contains an export-enabled private key.
cert-filename	The certificate file name that is located under the flash:.
key-filename	The private key file name that is located under the flash:.
password-text	Decryption password of private key file or decryption password of private key exported from PFX certificate.

【Default Configuration】-

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】Before executing this command to install the HTTPS service certificate, you need to put the certificate and/or private key files under the flash: partition through commands such as copy. After the installation is complete, you can delete the certificate/private key files under flash:.

You can delete the installed HTTPS service certificate with the no web-server https certificate command. After deletion, the HTTPS service will use a self-signed certificate.

This command does not appear in the configuration information (running-config).

After installing the HTTPS service certificate, the browser may require re-adding the trust of the certificate to continue accessing the web management of the device. It is recommended to close the browser and reopen the web management page.

【Configuration Example]】Install flash: Download the certificate file usercert.pfx, and export the password as 123456:

```
AC-FS#configure terminal
AC-FS(config)# web-server https certificate pfx usercert.pfx password 123456
*Feb 28 14:38:37: %HTTPD-4-CERT_CHANGE: HTTPS certificate changed.
% The certificate was successfully installed.
```

【Verification】Use show web-server https certificate information to view HTTPS service certificate information

【Prompt Information】1: If the certificate is installed successfully, the following prompt will be given:

```
% The certificate was successfully installed.
```

2: If the file name is greater than or equal to 64 bytes, the following prompt is given:

```
% Operation failed: filename too long, should be less than 64 bytes.
```

3: If the certificate and private key files do not match, give the following prompt:

% Operation failed: certificate does not matched with private key.

4: If the certificate file does not exist or the file is empty, the following prompt is given:

% Operation failed: certificate file not found or is empty.

5: If the private key file does not exist or the file is empty, the following prompt is given:

% Operation failed: private key file not found or is empty.

6: If the password is incorrect, the following prompt is given:

% Operation failed: please input correct password.

7: If the certificate file or private key file is parsed incorrectly, the following prompt is given:

% Operation failed: verify file failed.

8: If the certificate has not been installed but the delete certificate command is executed, the following prompt is given:

% Operation failed: no certificate installed.

9: If the deletion of the certificate is successful, the following prompt is given.

% The installed certificate was successfully deleted.

【Common Mistake】-

【Platform Description】 -

7.13 web-server https generate self-signed-certificate

Regenerate the HTTPS service self-signed certificate.

web-server https generate self-signed-certificate

【Parameter Description】-

【Default Configuration】 By default, the HTTPS service uses a self-signed certificate.

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 This command is an interactive command. After executing the command, you need to input the information required to generate a self-signed certificate according to the prompts, including the number of digits of the RSA key modulus and the certificate user name; or press Ctrl+C to abort the operation.

When a third-party HTTPS service certificate has been installed, the installed HTTPS service certificate will be used first, and regenerating a self-signed certificate will not replace the currently used HTTPS service certificate.

This command does not appear in the configuration information (running-config).

After regenerating the HTTPS service certificate, the browser may require re-adding trust in the certificate to continue accessing the web management of the device. It is recommended to close the browser and reopen the web management page.

【Configuration Example】Regenerate HTTPS service self-signed certificate

```
AC-FS#configure terminal
AC-FS(config)# web-server https generate self-signed-certificate
RSA key modulus bits (1024~4096) [2048]:
Common Name (e.g. server IP) [Self-Signed-600B16C2]:
% Generate self-signed certificate successfully.
```

【Verification】Use show web-server https certificate information to view HTTPS service certificate information

【Prompt Information】 1: If the input RSA key modulus length is not in the range of 1024~4096 or is not a number, the following information will be prompted:

```
% Invalid number.
```

2: If you press Ctrl+C when prompted for input, it will abort the operation, giving the following prompt:

```
% Operation cancelled.
```

3: If the entered certificate subject name exceeds 64 bytes, the following prompt will be given:

```
% Input too long, should not exceed 64 bytes.
```

4: If the self-signed certificate is successfully generated, the following prompt is given:

```
% Generate self-signed certificate successfully.
```

【Common Mistake】-

【Platform Description】 -

8 System log

8.1 clear logging

Clear the log information in the memory buffer.

clear logging

【Parameter Description】-

【Command Mode】 Privileged user mode

【Default Level】1

【Usage Guide】This command only clears the log message content in the memory buffer. The statistics of log packets cannot be cleared.

【Configuration Example]】1: The following example clears the log message content in the memory buffer.

```
AC-FS# clear logging
```

【Prompt Information】-

【Platform Description】 -

8.2 logging

Logs to the specified Syslog Server.

logging { ip-address | ipv6 ipv6-address } [udp-prot port]

Deletes the Syslog Server at the specified address from the Syslog Server list.

no logging { ip-address | ipv6 ipv6-address }

The default port number (514) for the Syslog Server to send recovery logs.

no logging { ip-address | ipv6 ipv6-address } udp-prot

【Parameter Description】

Parameter	Description
ip-address	The host IP address where the log information is received.

ipv6-address	Specifies the host IPV6 address that receives the log information..
udp-port port	Specify the port number for the log host (the default port number is 514)

【Default Configuration】 By default, no log information is sent to any Syslog Server.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command specifies a Syslog server to receive the log information of the device. Users can configure up to 5 Syslog Servers. Log information will be sent to all configured Syslog Servers simultaneously.

【Configuration Example]】1: The following example specifies a syslog server whose address is 202.101.11.1:

```
AC-FS(config)# logging 202.101.11.1
```

2: The following example specifies a syslog server with address 10.1.1.100 and port number 8099:

```
AC-FS(config)# logging 202.101.11.1 udp-port 8099
```

3: The following example specifies an IPV6 address as AAAA:BBBB::FFFF

```
AC-FS(config)# logging ipv6 AAAA:BBBB::FFFF
```

【Verification】1: Use the show logging command to view the set log server address.

【Prompt Information】 1: If there are more than 5 Syslog Servers configured on the device, an error will be prompted.

```
%%Warning: Can not configure more than 5 syslog servers!
```

【Common Mistake】-

【Platform Description】 -

8.3 logging buffered

Set the memory buffer parameters for logging log information (log information severity, buffer size).

logging buffered [buffer-size] [level]

Suppresses logging of log information in the memory buffer.

no logging buffered

Will restore the memory buffer size to the default value.

default logging buffered

Values range from 4K to 128K Bytes.

level The severity of the log message, from 0 to 7. Level names can be used, or numbers can be used directly.

【Parameter Description】

Parameter	Description
buffer-size	Buffer size, related to the specific device type: the value ranges from 4K to 128K Bytes.
level	The severity of the log message, from 0 to 7. Level names can be used, or numbers can be used directly.

【Default Configuration】 The default size of the buffer is related to the specific device type:

The default is 4K Bytes.

The log message severity defaults to 7.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 The memory buffer space is used circularly. If the memory area of the specified size is full, the earliest log information will be overwritten. To view log information for the memory buffer, use the privileged user command show logging.

The log information in the memory buffer is temporary. After the device is restarted or the privileged user command clear logging is executed, the log information in the buffer will be cleared. If you want to track down the problem, you should write the log to extended FLASH or send it to Syslog Server.

The log information is divided into the following 8 levels:

keywords	Grade	Description
Emergencies	0	In an emergency, the system cannot operate normally.
Alerts	1	Problems that require immediate measures to correct
Critical	2	punctum saliens
Errors	3	error message
Warnings	4	warning message

Notifications	5	Ordinary type, but important information.
Informational	6	Descriptive information
Debugging	7	Debug information

The smaller the value, the higher the level, that is, level 0 information is the highest level information.

After specifying the level of log information allowed to be displayed by the device, log information of the level equal to or lower than the set value will be allowed to be displayed.

After the system runs for a long time, modifying the log buffer size at this time, especially when the buffer is large, may not succeed, and a failure message will be displayed. This is generally because the system runs for a long time and there is not enough contiguous memory space available for allocation. It is recommended to modify the log buffer size when the system is just started.

【Configuration Example】1: The following example settings allow only log information with level 6 and below to be recorded in a memory buffer with a size of 10000 bytes:

```
AC-FS(config)# logging buffered 10000 6
```

【Verification】1: Use the show logging command to view the parameters of the set log memory buffer.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.4 logging console

Sets the level of log information allowed to be displayed on the console.

logging console [level]

Suppresses the printing of log messages on the console.

no logging console

【Parameter Description】

Parameter	Description
level	Severity of the log messages, ranging from 0 to 7. You can use the level name or the number directly character. For details of the severity of the log information, refer to the following [Usage Guide].

【Default Configuration】 7 (Debugging, debugging information)

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 After setting a log severity, log messages with values equal to or lower than the severity level will be displayed on the console. The related parameters and statistics of log settings can be viewed through the show logging command.

The log information is divided into the following 8 levels:

keywords	Grade	Description
Emergencies	0	In an emergency, the system cannot operate normally.
Alerts	1	Problems that require immediate measures to correct.
Critical	2	Important situation.
Errors	3	error message.
Warnings	4	warning message.
Notifications	5	Ordinary type, but important information.
Informational	6	Descriptive information.
Debugging	7	Debug information.

【Configuration Example]】1: The following example sets the level of log information allowed to be displayed in the console to 6:

```
AC-FS(config)# logging console informational
```

【Verification】1: Using the show logging command, you can view the level of log information that is allowed to be displayed on the console and the log entries that have been output to the console.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.5 logging count

Enable log statistics function.

logging count

Clear log statistics and turn off log statistics.

no logging count

【Parameter Description】-

【Default Configuration】 The log statistics function is disabled.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to open the log statistics function. Statistics start when the command is opened. When the no logging count command is executed, the statistics function is disabled and the statistics are cleared.

【Configuration Example]】1: Enable log statistics function:

```
AC-FS(config)# logging count
```

【Verification】1: Use the show logging command to check whether the log statistics function is enabled.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.6 logging delay-send file

The name of the log file cached locally on the device when the delayed upload is configured.

logging delay-send file flash:filename

When the delayed upload is resumed, the name of the log file cached locally on the device is the default value.

no logging delay-send file

【Parameter Description】

Parameter	Description

flash:filename	Delay the log file name.

【Default Configuration】 The default format of the log file name sent to the remote server is: file size_device IP address_index value.txt. If you modify the delayed file name, the log file name sent to the remote server is: The configured file name prefix_file size_device IP address_index value.txt; and the file name saved in the local Flash of the device is: configured file name prefix_index value.txt. The default filename prefix is: syslog_ftp_server.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command can be used to configure the log file name cached locally on the device during delayed upload.

The character period (.) cannot appear in the configured file name, because the file name will increase the index value and suffix when the system generates a local cache file (.txt), the index value is changed incrementally, and characters that are prohibited in PC file naming, such as: \/:*"<>| are not allowed.

For example: the file name configured by the user is log_server, the current file index value is 5, the file size is 1000B, and the IP address of the device sending the log file is 10.2.3.5, then the log file name of the sending remote server is: log_server_1000_10.2.3. 5_5.txt, but the log file name saved locally is log_server_5.txt.

If the IP address of the device sending the log file is in IPv6 form, because the IPv6 address may have a colon (:), and the colon (:) is the PC Characters that are forbidden in file naming, so need to be replaced by the character (-).

For example: the file name configured by the user is log_server, the file index value of Hanqian is 6, the file size is 1000B, and the IPv6 address of the device sending log files is 2001::1, then the log file name of the sending remote server is: log_server_1000_2001- 1_6.txt, but the log file name saved locally is log_server_6.txt.

【Configuration Example]】 1: Configure the log file name for delayed upload to be log_server:

```
AC-FS(config)# logging delay-send file flash:log_server
```

【Verification】 1: Use the show logging command to view the log file name cached locally on the device during delayed upload.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

8.7 logging delay-send interval

Configure the time interval for delaying log uploading to the server.

logging delay-send interval seconds

The time interval for delaying the upload of the recovery log to the server is the default value.

no logging delay-send interval

【Parameter Description】

Parameter	Description
seconds	Time interval for log delay on delivery (in seconds).

【Default Configuration】 The default time interval is 3600 seconds (1 hour).

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to set the time interval for the log delay to be sent to the server. The range that can be set is 600 ~ 65535, unit: second.

【Configuration Example]】1: The interval for delaying the upload of configuration logs is 600 seconds (1 minute):

```
AC-FS(config)# logging delay-send interval 600
```

【Verification】1: Use the show logging command to view the time interval for delayed log uploading.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.8 logging delay-send server

Configure the address and reporting method for delayed log uploading to the server.

logging delay-send server {ip-address | ipv6 ipv6-address } mode { ftp user username password

[0 | 7] password | tftp }

Delete the address and reporting method that logs are delayed to be sent to the server.

no logging delay-send server { ip-address | ipv6 ipv6-address }

【Parameter Description】

Parameter	Description
ip-address	The Server IP address that receives the log information.
ipv6 ipv6-address	The Server IPV6 address that receives the log information.
username	Specifies the user name of the ftp server.
password	Specify the password for the ftp server.
0	(Optional) The password is password graphic text.
7	Represents the subsequent password for simple encrypted ciphertext text.

【Default Configuration】 By default, no log information is sent to any FTP or TFTP Server.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command specifies an FTP or TFTP server to receive the log information of the device. The user can configure a total of 5 FTP or TFTP servers, and each server can only be configured with one of FTP or TFTP. The log information will be sent to all configured FTP or TFTP servers at the same time.

【Configuration Example]】1: The following example specifies an FTP Server whose address is 192.168.23.12, the user name is admin, and the password is admin:

```
AC-FS(config)# logging delay-send server 192.168.23.12 mode ftp user admin password admin
```

2: The following example specifies a TFTP Server with an IPV6 address of 2000::1:

```
AC-FS(config)# logging delay-send server ipv6 2000::1 mode tftp
```

【Verification】1: Use the show logging command to view the address and reporting method of the log delayed server.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.9 logging delay-send terminal

Enable delayed upload log output to console and remote terminal.

logging delay-send terminal

Turn off the delayed log output to the console and remote terminal.

no logging delay-send terminal

【Parameter Description】-

【Default Configuration】 By default, the delayed log output to the console and remote terminal is disabled.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 You can use this command to open the delayed log output to the console and remote terminal.

【Configuration Example]】1: The following example enables the delayed log output to the console and remote terminal:

```
AC-FS(config)# logging delay-send terminal
```

【Verification】1: Use the show logging command to view the switch status of the log output to the console and remote terminal.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.10 logging facility

Set the device value for log information

logging facility facility-type

The restore device value is the default value (23).

no logging facility

【Parameter Description】

Parameter	Description
facility-type	Syslog device value, refer to Usage Guide for specific set values.

【Default Configuration】 When the RFC5424 log format is enabled, the default value of the device is 16 (Local0, Local use); When the RFC5424 log format is not enabled, the device value defaults to 23 (Local7, Local use).

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 The device value of the log information is used to construct the priority of the log information. The specific calculation formula is:

priority = Facility (device value) * 8 + serverity (log level).

The calculated log priority will be sent to the log server as part of the log message. The log server can be used to identify different log sources, and to find and filter the logs corresponding to the log source.

The following table is the possible device values for Syslog:

Numerical Code	Facility
0 (kern)	Kernel messages
1 (user)	User-level messages
2 (mail)	Mail system
3 (daemon)	Syste daemons
4 (auth1)	security/authorization message
5 (syslog)	Messages generated internally by syslogd
6 (lpr)	Line printer system
7 (news)	USENET news
8 (uucp)	Unix-to-Unix copy system
9 (clock1)	Clock daemon
10 (auth2)	security/authorization message
11 (ftp)	FTP daemon
12 (ntp)	NTP daemon

13 (logaudit)	Log audit
14 (logalert)	Log alert
15 (clock2)	Clock daemon
16 (local0)	Local use
17 (local1)	Local use
18 (local2)	Local use
19 (local3)	Local use
20 (local4)	Local use
21 (local5)	Local use
22 (local6)	Local use
23 (local7)	Local use

The default device value is (local7)23.

【Configuration Example]】1: The following sets the Syslog device value as kernel:

```
AC-FS(config)# logging facility kern
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.11 logging file

Save the log information in a file, the log file can be saved in one of hard disk, extended FLASH, USB or SD card.

logging file { sata0:filename | flash:filename | flash2:filename | usb0:filename | usb1:filename | sd0:filename } [max-file-size] [level]

Cancel logging in extended FLASH.

no logging file

【Parameter Description】

Parameter	Description

sata0	The log file is selected to be saved on the hard disk.
flash	The log file selection is saved in the extended FLASH (when flash2 exists, the log file will be saved to flash2).
Flash2	Log file selection is saved in extended FLASH2.
usb0	The log file selection is saved in USB0, this option is only supported when the device has 1 USB interface, and an extended USB device is inserted.
usb1	The log file selection is saved in USB1, this option is only supported when the device has 2 USB ports, and an extended USB device is inserted.
sd0	The log file is selected to be saved in the SD card. This option is only supported when the device has an SD card interface, and an extended SD card device is inserted.
filename	Log file name. Without file type, it is fixed to txt type.
max-file-size	Maximum log file size. From 128K to 6M bytes, the default size is 128K.
level	The level of log information allowed to be logged to the log file. Level names can be used, or numbers can be used directly. The default log level for writing to extended FLASH is 6. For the level of log information, please refer to [Usage Guide].

【Default Configuration】 The log information cannot be recorded in the extended FLASH.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 If there is no Syslog Server, or you do not want to transmit log information in the network based on various security considerations, you can choose to save the log information directly in the extended FLASH.
The log file suffix is fixed to txt, and the configuration file suffix will be rejected.

To record the log information to the extended FLASH, the extended FLASH must be purchased separately. If the extended FLASH is not purchased, the logging file flash will be automatically hidden and configuration is not allowed. If there is no FLASH2, the logging file flash2 will be automatically hidden, and configuration is not allowed. When there is FLASH2, configure logging file flash, and log information will be recorded to FLASH2.

The log information is divided into the following 8 levels:

Keywords	Grade	Description
Emergencies	0	In an emergency, the system cannot operate normally.
Alerts	1	Problems that require immediate measures to correct

Critical	2	punctum saliens
Erro s	3	error message
Warnings	4	warning message
Notifications	5	Ordinary type, but important information.
Informational	6	Descriptive information
Debugging	7	Debug information

【Configuration Example]】1: The following example records the log information in the extended FLASH, the file name is syslog.txt, the file size is 128K, and the log information level is 6.

```
AC-FS(config)# logging file flash:syslog
```

【Verification】1: Use the show logging command to view the related parameters of the set log information saved in the extended FLASH.

【Prompt Information】 1: If the length of the log file name exceeds 20 characters during configuration, if the length of the file name during configuration is 21, an error will be prompted.

```
%Error: The file length must not be longer then 20, Current file length 21.
```

【Common Mistake】-

【Platform Description】 -

8.12 Logging file numbers

Configure the number of files written to the extended FLASH for system log information.

logging file numbers numbers

Unconfigure the number of log files and restore to the default value.

no logging file numbers

【Parameter Description】

Parameter	Description
numbers	Number of log files, range: 2~16, unit: individual.

【Default Configuration】 The default number of log files is 16.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to set the number of log files. You can use the no logging file numbers command to restore the number of log files to the default value of 16.

If the number of log files is modified, the system will not delete the log files that have been generated. Therefore, in order to save the space for expanding the FLASH, the user needs to manually delete the log files that have been generated by the system (the log files can be transmitted to the outside world through tftp before deletion). server). For example: After the system enables the log writing function, it will write 16 log files by default, and assuming that the device has generated 16 log files, and the number of log files to be modified is 2 at this time, the new log information generated by the system will be in the The two log files with index values of 0 and 1 are continuously covered and rewritten, but the log files with index values of 2 to 16 that have been generated before will still be retained, and the system will not delete them. Users can manually delete the logs according to their needs. document.

【Configuration Example]】1: The number of configuration log files in the following example is 8.

```
AC-FS(config)# logging file numbers 8
```

【Verification】1: Use the show run command to view the set number of log files.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.13 logging flash flush

Write the log information in the system buffer to the FLASH file immediately.

logging flash flush

【Parameter Description】-

【Default Configuration】-

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 After the system enables the log information writing function to FLASH file, the log information generated by the device will be cached in the system log buffer first. Only when the buffer is full or the timer expires, will the log in the buffer be stored The information is written into the FLASH file. You can set the log information in the system buffer to be immediately written into the FLASH file through this command.

When the user configures the logging flash flush command, the configuration works once, and the log information stored in the buffer is written to the FLASH file immediately after the configuration.

【Configuration Example]】1: The following example writes the log information in the system buffer to the FLASH file immediately.

```
AC-FS(config)# logging flash flush
```

【Verification】1: Use the dir command to view the log files written to FLASH.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.14 logging flash interval

Configure the time interval at which system log information is written to the extended FLASH.

logging flash interval seconds

Cancel the time interval for writing log information to FLASH and restore it to the default value.

no logging flash interval

【Parameter Description】

Parameter	Description
interval *seconds*	Time interval between log information written to FLASH file: 1~51840 in: seconds.

【Default Configuration】 The default interval for writing log information to the FLASH file is 3600s, that is: 1 hour.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to set the time interval for saving log information to the FLASH file, and start timing after the command is configured. You can run the no logging flash interval command to restore the interval for writing log information to the FLASH file to the default value of 3600s.

In order to prevent the system from writing FALSH files too frequently, the time interval should not be configured too small.

【Configuration Example]】1: The following example configures the time interval for writing log information to the FLASH file as 5 minutes (300s).

```
AC-FS(config)# logging flash interval 300
```

【Verification】1: Use the show logging command to view the parameters related to the set time interval.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.15 logging filter direction

Filter out log information going in a certain direction.

logging filter direction { all | buffer | file | server | terminal }

Clears the filter operation for log messages going in a certain direction.

no logging filter direction { all | buffer | file | server | terminal }

【Parameter Description】

Parameter	Description
all	Filter log information in all directions (including: Console direction, VTY terminal, log buffer, log file, log server).
buffer	Filters the log information to the log buffer (that is, that that is displayed by the show logging command).
file	Filter the log information to the log file.
server	Filters the log information to the log server.

terminal	Filter the log information to the console and VTY terminals (including Telnet / SSH, etc.).

【Default Configuration】 Filter the log information in all directions, that is, all

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 After the user configures the log filtering function, usually, they want to filter out the log information matching the filtering rules in all directions (including: Console direction, VTY terminal, log buffer, log file, log server) , and in some cases, the user may only want to filter log information in a specific direction. For example, the filtered log information does not need to be sent to the terminal interface, but needs to be written to the log file or sent to the log information device, and only needs to be configured Filter the log information in the terminal direction.

【Configuration Example]】1: The following example configures and filters log information in the terminal direction (including: console and VTY terminal, etc.):

```
AC-FS(config)# logging filter direction terminal
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.16 logging filter type

Configure the filter type of log information.

logging filter type { contains-only | filter-only }

The filter type of recovery log information.

no logging filter type

【Parameter Description】

Parameter	Description
contains-only	Include only, for exporting only logs containing the keywords information in the filtering rules, and other logs without the filtering rules do not output.
filter-only	Filter Only represents filtering out the logs that contain the keywords information in the filter rule and does not output these filtered out log information.

【Default Configuration】 The default filter type is "filter only".

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 1. In some cases, when there is too much log information from a certain module, it may cause the terminal interface to swipe, and when the user does not care about such log information, you can apply "Filter only" on the device ″This log filter type filters out the log information that is on the screen.

2. In some cases, users may only care about whether certain log information is generated, and the log filter type of "contain only" can be applied to the device, so that the log information containing this rule is output to the terminal interface, which is convenient to use. to observe whether certain events have occurred.

In the actual application process, the two filter types "include only" and "filter only" are mutually exclusive, that is, only one filter type can be configured at the same time.

During the configuration process, if only the filtering direction and filtering type are configured, but no filtering rule is configured, the configuration will not take effect, that is, the log filtering operation will not be performed.

【Configuration Example]】1: The following example configures the log information filter type to "include only":

```
AC-FS(config)# logging filter type contains-only
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.17 logging filter rule

Configure filtering rules for log information.

logging filter rule { exact-match module module-name mnemonic mnemonic-name level level |

single-match [level level | mnemonic mnemonic-name | module module-name] }

Delete the "exact match" filter rule for log information.

no logging filter rule exact-match [module module-name mnemonic mnemonic-name level level]

Delete the "single match" filter rule for log information.

no logging filter rule single-match [level level | mnemonic mnemonic-name | module module-name]

【Parameter Description】

Parameter	Description
exact-match	Exact match, if you choose exact match, the following three filter options need to be filled in.
single-match	Single match, if single match is selected, only one of the following three filter options needs to be filled in.
module module-name	Module name, that is, fill in the name of the module to be filtered.
mnemonic mnemonic-name	Mnemonic name, that is, fill in the mnemonic name of the log information to be filtered.
level level	Log information level, that is, fill in the log information level to be filtered.

【Default Configuration】 No log information filtering rules, no log filtering

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 1. In some cases, the user may only want to filter out a specific log information, you can use the "exact match" rule, when configuring, you need to specify the specific module name, mnemonic name, log grade.

2. In some cases, the user may want to filter out certain types of log information, then the "single match" rule can be used. When configuring, only one of the module name, log level, and mnemonic name needs to be specified.

In the log information filtering rule configured by the user, if the same module name, mnemonic or information level is configured in both the single matching rule and the exact matching rule, the single matching evasion has a higher priority than the exact matching.

【Configuration Example]】1: Configure the log information filtering rule as exact match, the module name is LOGIN, the log level is 5, and the mnemonic name is LOGOUT:

```
AC-FS(config)# logging filter rule exact-match module LOGIN mnemonic LOGOUT level 5
```

2: Configure the filter rule for log information to be a single match, and the module name is SYS:

```
AC-FS(config)# logging filter rule single-match module SYS
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.18 logging life-time

Configure the storage time of log files in extended FLASH.

logging life-time level level days

Unconfigure the log save time.

no logging life-time level level

【Parameter Description】

Parameter	Description
level	Specify the log information level, either use the level name or numbers directly.
days	Days of log file saves corresponding to the log information level.

【Default Configuration】 By default, there is no limit on the storage time of log files. The storage time of log files is limited by the size of the log file configured by the user.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Considering the size of the extended FLASH and the importance of different levels of log information, you can specify different storage days for different levels of log information.

When the user enables the time-based log saving function, the original file size-based log saving function will be invalid, and the log information files will be uniformly stored in the syslog/ directory of the extended FLASH.

【Configuration Example]】 1: The following example configures log information with log information level 6 and saves it for 10 days:

```
AC-FS(config)# logging life-time level 6 10
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

8.19 logging monitor

Sets the level of log information allowed to be displayed on VTY windows (Telnet windows, SSH windows, etc.).

logging monitor [level]

Disables the printing of log messages on the VTY window.

no logging monitor

【Parameter Description】

Parameter	Description
level	Severity of log packets. Level names can be used, or numbers can be used directly. For a detailed description of the severity of log messages, please refer to [Usage Guide].

【Default Configuration】 Allows the level of log information displayed on the VTY window to be 7 (Debugging, debugging information)

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 To print log information on the VTY window, first execute the privileged user command terminal monitor to allow the log information to be printed in the current VTY window. Then you can execute the global configuration mode command logging monitor to define the level of log information displayed on the VTY window.

The log information is divided into the following 8 levels:

Keywords	Grade	Description
Emergencies	0	In an emergency, the system cannot operate normally.
Alerts	1	Problems that require immediate measures to correct.
Crit cal	2	punctum saliens.
Errors	3	error message.
Warnings	4	warning message.
Notifications	5	Ordinary type, but important information.
Informational	6	Descriptive information.
Debugging	7	Debug information.

【Configuration Example]】1: The following example configures the level of log information that can be printed on the VTY window to be 6:

```
AC-FS(config)# logging monitor informational
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.20 logging on

Allows the display of log information on different devices.

logging on

Display of log information is prohibited.

no logging on

【Parameter Description】-

【Default Configuration】 Allow log information to be displayed on different devices.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Log information can not only be displayed on Console window, VTY window, but also recorded on different devices: memory buffer, extended FLASH, Syslog Server. This command is the general log switch. If the log switch is turned off, all log information will not be displayed or recorded, except for Logs with a severity level greater than 1.

【Configuration Example]】1: The following example turns off the log switch on the device:

```
AC-FS(config)# no logging on
```

【Verification】1: Use the show logging command to check whether the log information is allowed to be displayed on the device.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.21 logging policy

Configure the classification policy used for log classification reporting.

logging policy module module-name [not-lesser-than] level direction { all | server | file | console | monitor | buffer }

Delete a classification policy for log classification reporting.

no logging policy module module-name [not-lesser-than] level direction { all | server | file | console | monitor | buffer }

Delete the classification policy for all log classification reports.

no logging policy

【Parameter Description】

Parameter	Description
module-name	The module name of the grading strategy.

not-lesser-than	When this option is specified, logs with a log level greater than or equal to the configured log level will be output in the configured direction, and logs with a log level less than the configured log level will be filtered out; When this option is not specified, logs with a log level less than or equal to the configured log level will be output in the configured direction, and logs with a log level greater than the configured log level will be filtered out.
level	The log level of the classification policy to be configured.
all	Enforce log classification policies in all directions.
server	Only implement the log classification policy in the direction of sending to the log server.
file	Only implement the log classification policy in the direction of output to the log file.
console	Only implement the log classification policy in the direction of output to the console.
monitor	Only implement the log classification policy in the direction of output to the remote terminal.
buffer	Only implement the log classification policy in the direction of saving to the buffer.

【Default Configuration】 By default, the log classification policy is not implemented.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command is used to configure log output to different destinations by module and severity level.

【Configuration Example]】1: Configure the logs of the SYS module level greater than or equal to level 5 to be output only to the console, and the logs of level less than or equal to level 3 to be output only to the buffer direction:

```
AC-FS(config)# logging policy module SYS not-lesser-than 5 direction console
AC-FS(config)# logging policy module SYS 3 direction buffer
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.22 logging rate-limit

Enable the log rate limit function to limit the log information that is allowed to be output per second.

logging rate-limit { number | all number | console { number | all number } } [except [severity]]

Turn off log rate limiting.

no logging rate-limit

【Parameter Description】

Parameter	Description
number	The log information allowed to be processed in one second, the range is 1~10000.
all	Set the rate control for all log information, including all log information of level 0~7.
console	Sets the number of log messages allowed to be displayed on the console per second.
except	Log information with a severity level less than or equal to this level does not perform rate control; the default level is error(3), and rate control is not performed on log information with a level less than or equal to error.
severity	Severity level of log information. The lower the level, the higher the severity. The range is 0~7.

【Default Configuration】 Rate control is not performed.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command controls the log information output of the system. Using this command can prevent the output of a large amount of log information.

【Configuration Example]】1: Set all log messages (including debug) that are allowed to be processed per second to 10, but do not control warning and higher severity levels:

```
AC-FS(config)#logging rate-limit all 10 except warnings
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.23 logging server

Logs to the specified Syslog Server.

logging server { ip-address | ipv6 ipv6-address } [udp-prot port]

Deletes the Syslog Server at the specified address from the Syslog Server list.

no logging server { ip-address | ipv6 ipv6-address }

The default port number (514) for the Syslog Server to send recovery logs.

no logging server { ip-address | ipv6 ipv6-address } udp-prot

【Parameter Description】

Parameter	Description
ip-address	The host IP address where the log information is received.
ipv6-address	Specifies the host IPV6 address that receives the log information.
udp-port port	Specify the port number for the log host (the default port number is 514).

【Default Configuration】 By default, no log information is sent to any Syslog Server.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command specifies a Syslog server to receive the log information of the device. Users can configure up to 5 Syslog Servers. Log information will be sent to all configured Syslog Servers simultaneously.

Ipv6 server does not support vrf and oob.

【Configuration Example]】1: The following example specifies a syslog server whose address is 202.101.11.1:

```
AC-FS(config)# logging server 202.101.11.1
```

2: The following example specifies a syslog server with address 10.1.1.100 and port number 8099:

```
AC-FS(config)# logging server 202.101.11.1 udp-port 8099
```

3: The following example specifies an IPV6 address as AAAA:BBBB::FFFF

```
AC-FS(config)# logging server ipv6 AAAA:BBBB::FFFF
```

【Verification】 1: Use the show logging command to view the set log server address.

【Prompt Information】 1: If there are more than 5 Syslog Servers configured on the device, an error will be prompted.

```
%%Warning: Can not configure more than 5 syslog servers!
```

【Common Mistake】 -

【Platform Description】 -

8.24 logging source interface

Set the source interface of log packets.

logging source [interface] interface-type interface-number

Cancel the source interface setting of the specified packet.

no logging source [interface]

【Parameter Description】

Parameter	Description
interface-type	interface type.
interface-number	Interface number.

【Default Configuration】 The log source address is not set by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 By default, the source IP address of log packets sent to the Syslog Server is the IP address of the interface that sends the packets. To facilitate tracking and management, this command can be used to fix the source IP address of all log packets to the IP address of an interface, so that the administrator can identify the log packets sent from which device through the unique address. If the source interface is configured or no IP address is configured on the source interface, the source IP address of log packets is still the IP address of the interface that sends the packets.

【Configuration Example]】1: The following example specifies the address of Loopback 0 as the source address of Syslog packets:

```
AC-FS(config)# logging source interface loopback 0
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.25 logging source ip | ipv6

Set the source IP address of log packets.

logging source { ip ip-address | ipv6 ipv6-address }

Cancel the source IP address setting of the specified packet.

no logging source { ip | ipv6 }

【Parameter Description】

Parameter	Description
ip-address	Specifies the source IPV4 address that sends a log message to the IPV4 log host.
ipv6-address	Specifies the source IPV6 address that sends a log message to the IPV6 log host.

【Default Configuration】 The log source address is not set by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 By default, the source IP address of log packets sent to the Syslog Server is the IP address of the interface that sends the packets. In order to facilitate tracking and management, you can use this command to fix the source IP address of all log packets to a certain IP address, so that the administrator can identify the log packets sent from which device through the unique address. IP address, the source IP address of log packets is still the IP address of the interface that sends the packets.

【Configuration Example]】1: The following example specifies the address 192.168.1.1 as the source address of Syslog packets:

```
AC-FS(config)# logging source ip 192.168.1.1
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.26 logging statistic enable

Enable the log timing upload function.

logging statistic enable

Disable the scheduled log upload function.

no logging statistic enable

【Parameter Description】-

【Default Configuration】 The default is to disable the log timing upload function.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】You can use this command to enable the log timing upload function. After the log timing upload function is enabled, the system will output a series of performance statistics at certain time intervals, which is convenient for the log server to track the performance of the system.

【Configuration Example]】1: The following example enables the function of log timing upload:

```
AC-FS(config)# logging statistic enable
```

【Verification】1: Use the show logging command to view the on/off status of the log timing upload function.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.27 Logging statistic interval

Configure the interval for regular log uploading.

logging statistic mnemonic mnemonic interval minutes

Restore the default log upload interval.

no logging statistic mnemonic mnemonic

【Parameter Description】

Parameter	Description
mnemonic	A mnemonic string sent on log timing to identify system performance statistics objects
minutes	Time interval of regular delivery, unit: minutes

【Default Configuration】 The default time interval for scheduled upload is 15 minutes.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 You can use this command to configure the time interval for periodic reporting of a performance statistics object in the system. The time interval that can be set is 0, 15, 30, 60, 120 minutes, where 0 means to turn off the scheduled upload function of this statistic object.

【Configuration Example]】1: The following example sets the time interval for the scheduled upload of the statistics object TUNNEL_STAT to 30 minutes:

```
AC-FS(config)# logging statistic mnemonic TUNNEL_STAT interval 30
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.28 logging statistic terminal

Enable scheduled log upload (system performance statistics log) to output to the console and remote terminal.

logging statistic terminal

Turn off the scheduled log output to the console and remote terminal.

no logging statistic terminal

【Parameter Description】-

【Default Configuration】 By default, the log output to the console and remote terminal is disabled.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 You can use this command to open the log output to the console and remote terminal.

【Configuration Example]】1: The following example enables the scheduled log output to the console and remote terminal:

```
AC-FS(config)# logging statistic terminal
```

【Verification】1: Use the show logging command to view the switch status of the log output to the console and remote terminal at regular intervals.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.29 logging synchronous

Enable the synchronization of user input and log information output to prevent interruptions when users are typing characters.

logging synchronous

Disable the synchronization of user input and log information output.

no logging synchronous

【Parameter Description】-

【Default Configuration】 The synchronization function of user input and log information output is disabled

【Command Mode】Line configuration mode

【Default Level】 14

【Usage Guide】 This command enables the function of synchronizing user input and log information output, which can prevent the characters being input by the user from being interrupted, such as the following usage: The command will re-output:

```
AC-FS# configure terminal
Oct  9 23:40:55 %LINK-5-CHANGED: Interface GigabitEthernet 0/1, changed state to down
Oct  9 23:40:55 %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/1, changed state to DOWN
AC-FS# configure terminal      / / User-entered commands are re-output without interruption
```

【Configuration Example】】1: The following command enables the synchronization of user input and log information output on the console:

```
AC-FS(config)#line console 0
AC-FS(config-line)#logging synchronous
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.30 logging trap

Sets the level of log information allowed to be sent to the Syslog Server.

logging trap [level]

It is forbidden to send log messages to Syslog Server.

no logging trap

【Parameter Description】

Parameter	Description
level	Severity of log packets. Level names can be used, or numbers can be used directly. For a detailed description of the severity of log messages, please refer to the [Usage Guide].

【Default Configuration】 6 (Informational, Description information).

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 To send log information to the Syslog Server, first configure the Syslog Server using the global configuration command logging. Then, use the logging trap to specify the severity level sent to the log messages.

The related parameters and statistics of log settings can be viewed through the show logging command.

The log information is divided into the following 8 levels:

Keywords	Grade	Description
mergencies	0	In an emergency, the system cannot operate normally.
Alerts	1	Issues that require immediate action to correct
Critica	2	important situation
Errors	3	error message
Warnings	4	Warning message
Notifications	5	Common type, but important information to pay attention to.

Informational	6	descriptive information
Debugging	7	debug info

【Configuration Example】1: The following example configures the log information of level 6 to be sent to the Syslog Server whose address is 202.101.11.22:

```
AC-FS(config)# logging server 202.101.11.22
AC-FS(config)# logging trap informational
```

【Verification】1: Use the show logging command to view the set log information level that is allowed to be sent to the Syslog Server.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.31 logging userinfo

Enable logging of user login/logout log information.

logging userinfo

Turn off the log information that records user login/logout.

no logging userinfo

【Parameter Description】-

【Default Configuration】 When the user logs in/out of the device, the device will not record the related log information.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 After enabling the log information for logging in/out of the device, when a user connects to the device, the corresponding log information will be displayed to remind the device administrator. The log format is as follows:

Mar 22 14:05:45 %LOGIN-5-LOGIN_SUCCESS: User login from vty0 (192.168.23.68) OK.

【Configuration Example]】1: The following example configures the log information function to enable logging in/out of the device:

```
AC-FS(config)# logging user-info
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.32 logging userinfo command-log

Enable Log information for recording user actions.

logging userinfo command-log

Turn off the Log information that records user actions.

no logging userinfo command-log

【Parameter Description】-

【Default Configuration】 The device will not record the log information of related operations.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】After enabling the log information for recording user operations, when a user modifies the device configuration, the corresponding log information will be displayed to remind the device administrator. The log format is as follows:

```
Mar 22 14:10:40 %CLI-5-EXEC_CMD: Configured from vty0 (192.168.23.68) command-log: logging server
192.168.23.68.
```

【Configuration Example]】1: The following example configures the log information function to record user operations:

```
AC-FS(config)# logging user-info command-log
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.33 service log-format rfc5424

Switch to RFC5424 log format.

service log-format rfc5424

Switch to the old log format.

no service log-format rfc5424

【Parameter Description】-

【Default Configuration】 By default, the old log format (ie RFC3164 log format) is used.

【Command Mode】 Global configuration mode

【Default Level】 14

【 Usage Guide 】After switching to the RFC5424 log format, the commands service sequence-numbers, service sysname, service timestamps, service private-syslog, and service standard-syslog in the old log format will be invalid and hidden.

Switching to the old log format, the commands logging delay-send, logging policy, logging statistic used in the RFC5424 log format will be disabled and hidden.

The display contents of the show logging and show logging config commands will also change before and after the switch between the old and new log formats.

【Configuration Example]】1: The following example configures the log format as RFC5424 log format:

```
AC-FS(config)# service log-format rfc5424
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.34 service private-syslog

Adjust the log format to a private log display format.

service private-syslog

Cancel the private log display format and use the default log format for display.

no service private-syslog

【Parameter Description】-

【Default Configuration】 The log information is displayed in the default log format.

【Command Mode】 Global configuration mode

【Default Level】 14

【 Usage Guide 】 By default, the log information on the device is displayed in the following format: *timestamp: %facility-severity-mnemonic: description

The order is: * timestamp: % module name - severity level - mnemonic information: detailed log information examples are:

```
*May 31 23:25:21: %SYS-5-CONFIG_I: Configured from console by console
```

If the private log format display function is enabled, the log information display format on the device is as follows:

timestamp facility-severity-mnemonic: description

The order is: timestamp module name - severity level - mnemonic information: detailed log information examples are:

```
May 31 23:31:28 SYS-5-CONFIG_I: Configured from console by console
```

Among them, the difference between the private log format and the default log format lies in the timestamp and the identification string. The timestamp of the private log format is missing a "*" in the front, a ":" in the back, and a "%" in the front of the identification string. "

【Configuration Example]】1: The following example configuration adjusts the log format to a private log format

```
AC-FS(config)# service private-syslog
```

【Verification】1: Use the show logging command to check whether the log display format is adjusted to a private format.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.35 service sequence-numbers

Add serial number to log information

service sequence-numbers

Cancel the sequence number in the log message.

no service sequence-numbers

【Parameter Description】-

【Default Configuration】 There is no serial number in the log information.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】In addition to adding timestamp information to log information, you can also add serial numbers to log information, starting from 1. After adding the serial number, you can know very clearly whether the log information is lost and the order in which the logs are generated.

【Configuration Example]】1: The following example configuration adds a serial number to the log information:

```
AC-FS(config)# service sequence-numbers
```

【Verification】1: Use the show logging command to check whether the log format has a sequence number added.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.36 service standard-syslog

Adjust the log format to the log format defined in the standard RFC3164.

service standard-syslog

Cancel the log format defined in the standard RFC3164, and use the default log format for display.

no service standard-syslog

【Parameter Description】-

【Default Configuration】 The log information is displayed in the default log format.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 By default, the log information display format on the device is as follows:

*timestamp: %facility-severity-mnemonic: description

The order is: * timestamp: % module name - severity level - mnemonic information: detailed log information examples are:

*May 31 23:25:21: %SYS-5-CONFIG_I: Configured from console by console

If the standard log format display function is enabled, the log information display format on the device is as follows:

timestamp %facility-severity-mnemonic: description

The order is: timestamp % module name - severity level - mnemonic information: For example, detailed log information:

May 31 23:31:28 %SYS-5-CONFIG_I: Configured from console by console

Among them, the difference between the standard log format and the default log format is the timestamp. The timestamp of the standard log format is missing a "*" in the front and a ":" in the back.

【Configuration Example]】1: The following example configuration adjusts the log format to the standard log format

AC-FS(config)# service standard-syslog

【Verification】1: Use the show logging command to check whether the log display format is adjusted to the standard format.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.37 service sysname

Add the system name to the log information.

service sysname

Suppresses the system name in the log message.

no service sysname

【Parameter Description】-

【Default Configuration】 The system name is not included in the log information.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 In addition to adding timestamp information to log information, you can also add system name to log information. After adding the system name, after the log is sent to the server, on the server, you can clearly know which device the log information comes from.

【Configuration Example]】1: The following example configuration adds the system name to the log information:

```
Mar 22 15:28:02 %SYS-5-CONFIG: Configured from console by console
AC-FS# config terminal
Enter configuration commands, one per line. End with CNTL/Z. AC-
FS(config)# service sysname
AC-FS(config)# end
Mar 22 15:35:57 AC-FS %SYS-5-CONFIG: Configured from console by console
```

【Verification】1: Use the show logging command to check whether the system name is added to the log format.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.38 service timestamps

Add timestamp information to log information.

service timestamps [message-type [uptime | datetime [msec | year]]]

Cancel the time stamp information in the log information.

no service timestamps [message-type]

The timestamp of the recovery log information is the default value.

default service timestamps [message-type]

【Parameter Description】

Parameter	Description
message-type	L Log type, there are two kinds of log and debug. The log information refers to the log information with the severity level between 0 and 6, and the debug information refers to the log information with the severity level 7.
uptime	Device start time, format: * day and * hour * minutes and * seconds, example: 07:00:10:41
datetime	Current device date, format: Month Date: minutes: seconds, Example: Jul 27 16:53:07
msec	Current device date supports millisecond display, format: month date: minutes: seconds. millisecond example: Jul 27 16:53:07.299
year	Current device date support year display, format: year month Date time: minute: seconds example: 2007 Jul 27 16:53:07

【Default Configuration】 The timestamp in the log information is the current device time. If the device does not have an RTC, it is automatically adjusted to the device boot time.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 The time format of using the Uptime option is the running time of the device since the last startup to the present, in

seconds. The time format using the Datetime option is the current device date, year-month-day hours: minutes: seconds.

【Configuration Example]】1: The following example configures the timestamp to enable Log information and Debug information, the format is Datetime:, and supports millisecond display:

```
AC-FS(config)# service timestamps debug datetime msec
AC-FS(config)# service timestamps log datetime msec AC-
FS(config)# end
Oct 8 23:04:58.301 %SYS-5-CONFIG_I: Configured from console by console
```

【Verification】1: Use the show logging command to view the log timestamp format type.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

8.39 show logging

View log configuration parameters, statistics, and log packets in the memory buffer. Log information is displayed in order from oldest to newest timestamp.

show logging

【Parameter Description】-

【Command Mode】 Privileged user mode

【Default Level】1

【Usage Guide】-

【Configuration Example]】1: The following example is a result of executing show logging without enabling the RFC5424 log format:

```
AC-FS# show logging
Syslog logging: enabled
  Console logging: level debugging, 15495 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 15496 messages logged
  Standard format: false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: enable
  Sysname log messages: enable
  Count log messages: enable
  Trap logging: level informational, 15242 message lines logged,0 fail
    logging to  202.101.11.22
    logging to  192.168.200.112
Log Buffer (Total 131072 Bytes): have written 1336,
015487: *Sep 19 02:46:13: AC-FS %LINK-3-UPDOWN: Interface FastEthernet 0/24, changed state to up.
015488: *Sep 19 02:46:13: AC-FS %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 0/24,
changed state to up.
015489: *Sep 19 02:46:26: AC-FS %LINK-3-UPDOWN: Interface FastEthernet 0/24, changed state to down.
015490: *Sep 19 02:46:26: AC-FS %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 0/24,
changed state to down.
015491: *Sep 19 02:46:28: AC-FS %LINK-3-UPDOWN: Interface FastEthernet 0/24, changed state to up.
015492: *Sep 19 02:46:28: AC-FS %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 0/24,
changed state to up.
```

Field Description:

Field	Description
Syslog logging	Log switch: Turn on display enabled and turn display disabled off.
Console logging	The level of log information printed on the console, as well as the statistics.
Monitor logging	The level of journal interest for printing on the VTY window, and the statistics.
Buffer logging	The level of log information logged in the memory buffer, and the statistics.
Standard format	Standard log format.
Timestamp debug messages	Debug Information timestamp format.
Timestamp log messages	Log Information timestamp format.

Sequence-number log messages	Serial number switch.
Sysnam log messages	Add the system name to the log information.
Count log messages	Logging statistics function.
Trap lo ging	Level of information sent to the Syslog Server log information, and statistics.
Log Buffer	A log message logged in the memory buffer.

2: The following example is a result of executing show logging when the RFC5424 log format is enabled:

```
AC-FS# show logging
Syslog logging: enabled
  Console logging: level debugging, 4740 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 4745 messages logged
  Statistic log messages: disable
  Statistic log messages to terminal: disable
  Delay-send file name:syslog_ftp_server, Current write index:3, Current send index:3, Cycle:10
seconds
  Count log messages: enable
  Trap logging: level informational, 2641 message lines logged,4155 fail
    logging to  192.168.23.89
    logging to  2000::1
  Delay-send logging: 2641 message lines logged
    logging to  192.168.23.89  by tftp
Log Buffer (Total 4096 Bytes): have written 4096, Overwritten 3292
<135>1 2013-07-24T12:19:33.130290Z AC-FS - 7------- Please config the IP address for capwap.
<132>1 2013-07-24T12:20:02.80313Z AC-FS CAPWAP 4 NO_IP_ADDR   No ip address for capwap.
<135>1 2013-07-24T12:20:02.80343Z AC-FS - 7------- Please config the IP address for capwap.
<132>1 2013-07-24T12:20:32.250265Z AC-FS CAPWAP 4 NO_IP_ADDR   No ip address for capwap.
<134>1 2013-07-24T12:29:33.410123Z AC-FS SYS 6 SHELL_LOGIN [USER@4881 name="" type=""
from="console"] user login success.
<134>1 2013-07-24T12:29:34.343763Z AC-FS SYS 6 SHELL_CMD [USER@4881 name=""][CMD@4881
task="rl con" cmd="enable"]
```

Field Description:

Field	Description

Syslog logging	Log switch: open display enabled, close display disabled.
Console logging	The level of log information printed on the console, along with statistics.
Monitor logging	The level of log information printed on the VT window, along with statistics.
Buffer logging	The level of log information recorded in the memory buffer, and statistics.
Count log messages	Log statistics function.
Statistic log messages	The main switch of the log timing upload function.
Statistic log messages to terminal	The switch for the log to be regularly uploaded to the output console and remote terminal.
Delay-send file ame	The log delay uploads the file name cached locally on the device, the currently written file index, and the time interval for delayed uploading.
Trap logging	Level of log messages sent to Syslog Server, and statistics.
Delay-send logging	The address and upload method of the log delayed to the server, and statistics.
Log Buffer	Log messages recorded in the memory buffer.

【Prompt Information】-

【Platform Description】 -

8.40 show logging config

View the parameters and statistics of the log configuration.

show logging config

【Parameter Description】-

【Command Mode】 Privileged user mode

【Default Level】1

【Usage Guide】-

【Configuration Example】1: The following example is a result of executing show logging config without enabling the RFC5424 log format:

```
AC-FS# show logging config
Syslog logging: enabled
  Console logging: level debugging, 15495 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 15496 messages logged
  Standard format: false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: enable
  Sysname log messages: enable
  Count log messages: enable
  Trap logging: level informational, 15242 message lines logged,0 fail
    logging to  202.101.11.22
    logging to  192.168.200.112
```

Field Description:

Field	Description
Syslog logging	Log switch: open display enabled, close display disabled.
Console logging	The level of log information printed on the console, along with statistics.
Monitor logging	The level of log information printed on the VTY window, along with statistics.
Buffer logging	The level of log information recorded in the memory buffer, and statistics.
Standard format	Standard log format.
Timestamp debug messages	Debug information timestamp format.
Timestamp log messa es	Log information timestamp format.
Sequence-number log messages	serial number switch.
Sysname log messages	Add the system name to the log information.
Count log messages	Log statistics function.
Trap logging	Level of log messages sent to Syslog Server, and statistics.

2: The following example is a result of executing show logging config when the RFC5424 log format is enabled:

```
AC-FS# show logging
Syslog logging: enabled
  Console logging: level debugging, 4740 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 4745 messages logged
  Statistic log messages: disable
  Statistic log messages to terminal: disable
  Delay-send file name:syslog_ftp_server, Current write index:3, Current send index:3, Cycle:10
seconds
  Count log messages: enable
  Trap logging: level informational, 2641 message lines logged,4155 fail
    logging to  192.168.23.89
    logging to  2000::1
  Delay-send logging: 2641 message lines logged
    logging to  192.168.23.89  by tftp
```

Field Description:

Field	Description
Syslog logging	Log switch: open display enabled, close display disabled.
Console logging	The level of log information printed on the console, along with statistics.
Monitor logging	The level of log information printed on the VTY window, along with statistics.
Buffer logging	The level of log information recorded in the memory buffer, and statistics.
Count log messages	Log statistics function.
Statistic log messages	The main switch of the log timing upload function.
Statistic log messages to terminal	The switch for the log to be regularly uploaded to the output console and remote terminal.
Delay-send file name	Log delayed uploading of the file name cached locally on the device, the currently written file index, and the time interval for delayed uploading.
Trap logging	Level of log messages sent to Syslog Server, and statistics.
Delay-send logging	The address and upload method of the log delayed to the server, and statistics.

【Prompt Information】-

【Platform Description】 -

8.41 show logging count

View the number of times the log information of each module in the system is generated, as well as the last generated time and other statistical information.

show logging count

【Parameter Description】-

【Command Mode】 Privileged user mode

【Default Level】1

【Usage Guide】 To use the log packet statistics function, you need to execute the logging count command in the global configuration mode. After the log packet statistics function is enabled, the log packets output from the system will be classified and counted, and the statistics results can be viewed by running the show logging count command.

【Configuration Example]】1: The following example is the result of executing show logging count:

```
AC-FS# show logging count
Module Name   Message Name Sev Occur      Last Time
==================================================SYS            CONFIG_I         5          1
Jul 6 10:29:57
──────────────────────────────────────────── SYS       TOTAL      1
```

Field Description:

Field	Description
Module Name	log module name.
Message Name	log mnemonic name.
Sev	log level.
Occur	Log entries of this type counted since logging count was turned on.
Last Time	The last time such a log was generated.

【Prompt Information】-

【Platform Description】 -

8.42 show logging reverse

View log configuration parameters, statistics, and log packets in the memory buffer. Log information is displayed in order from newest to oldest timestamp.

show logging reverse

【Parameter Description】-

【Command Mode】 Privileged user mode

【Default Level】1

【Usage Guide】-

【Configuration Example】1: The following example is a result of executing show logging reverse without enabling the RFC5424 log format:

```
AC-FS# show logging reverse
Syslog logging: enabled
  Console logging: level debugging, 15495 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 15496 messages logged
  Standard format: false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: enable
  Sysname log messages: enable
  Count log messages: enable
  Trap logging: level informational, 15242 message lines logged,0 fail
    logging to  202.101.11.22
    logging to  192.168.200.112
Log Buffer (Total 131072 Bytes): have written 1336,
015492: *Sep 19 02:46:28: AC-FS %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 0/24,
changed state to up.
015491: *Sep 19 02:46:28: AC-FS %LINK-3-UPDOWN: Interface FastEthernet 0/24, changed state to up.
```

```
015490: *Sep 19 02:46:26: AC-FS %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 0/24,
changed state to down.
015489: *Sep 19 02:46:26: AC-FS %LINK-3-UPDOWN: Interface FastEthernet 0/24, changed state to down.
015488: *Sep 19 02:46:13: AC-FS %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 0/24,
changed state to up.
015487: *Sep 19 02:46:13: AC-FS %LINK-3-UPDOWN: Interface FastEthernet 0/24, changed state to up.
```

Field Description:

Field	Description
Syslog logging	Log switch: open display enabled, close display disabled.
Console logging	The level of log information printed on the console, along with statistics.
Monitor logging	The level of log information printed on the VTY window, along with statistics.
Buffer logging	The level of log information recorded in the memory buffer, and statistics.
Standard format	Standard log format.
Timestamp debug messages	Debug information timestamp format.
Timestamp log messages	Log information timestamp format.
Sequence-number log messages	serial number switch.
Sysname log messages	Add the system name to the log information.
Count log messages	Log statistics function.
Trap logging	Level of log messages sent to Syslog Server, and statistics.
Log Buffer	Log messages recorded in the memory buffer.

2: The following example is a result of executing show logging reverse when the RFC5424 log format is enabled:

```
AC-FS# show logging reverse
Syslog logging: enabled
  Console logging: level debugging, 4740 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 4745 messages logged
  Statistic log messages: disable
  Statistic log messages to terminal: disable
  Delay-send file name:syslog_ftp_server, Current write index:3, Current send index:3, Cycle:10
seconds
  Count log messages: enable
  Trap logging: level informational, 2641 message lines logged,4155 fail
    logging to  192.168.23.89
    logging to  2000::1
  Delay-send logging: 2641 message lines logged
```

```
    logging to  192.168.23.89  by tftp
Log Buffer (Total 4096 Bytes): have written 4096, Overwritten 3292
<134>1 2013-07-24T12:29:34.343763Z AC-FS SYS 6 SHELL_CMD [USER@4881 name=""][CMD@4881
task="rl_con" cmd="enable"]
<134>1 2013-07-24T12:29:33.410123Z AC-FS SYS 6 SHELL_LOGIN [USER@4881 name="" type=""
from="console"] user login success.
<132>1 2013-07-24T12:20:32.250265Z AC-FS CAPWAP 4 NO_IP_ADDR - No ip address for capwap.
<135>1 2013-07-24T12:20:02.80343Z AC-FS - 7------- Please config the IP address for capwap.
<132>1 2013-07-24T12:20:02.80313Z AC-FS CAPWAP 4 NO_IP_ADDR   No ip address for capwap.
<135>1 2013-07-24T12:19:33.130290Z AC-FS - 7------- Please config the IP address for capwap.
```

Field Description:

Field	Description
Syslog logging	Log switch: open display enabled, close display disabled.
Console logging	The level of log information printed on the console, along with statistics.
Monitor logging	The level of log information printed on the VTY window, along with statistics.
Buffer logging	The level of log information recorded in the memory buffer, and statistics.
Count log messages	Log statistics function.
Statistic log messages	The main switch of the log timing upload function.

Statistic log messages to terminal	The switch for the log to be regularly uploaded to the output console and remote terminal.
Delay-send file name	The log is delayed to upload the file name cached locally on the device, the currently written file.
Trap logging	file index and the time interval for delayed uploading.
Delay-send logging	Level of log messages sent to Syslog Server, and statistics.
Log Buffer	The address and upload method of the log delayed to the server, and statistics.

【Prompt Information】-

【Platform Description】 -

8.43 terminal monitor

Allows log information to be displayed on the current VTY window.

terminal monitor

Turn off displaying log messages on the current VTY window.

terminal no monitor

【Parameter Description】-

【Default Configuration】 The log information is not allowed to be displayed on the VTY window.

【Command Mode】 Privileged user mode

【Default Level】 14

【Usage Guide】 This command only sets the temporary properties of the current VTY. As a temporary property setting, it will not be saved permanently. After the VTY terminal session ends, the default settings are used and the temporary property settings are invalid. The command can also be executed on the console, but it doesn't work.

【Configuration Example】1: In the following example, set the current VTY window to allow printing of log information.

```
AC-FS# terminal monitor
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

9 RLOG

1.1ip nat-log on

Enable logging of local NAT only.

ip nat-log on

Close SSM.

no ip nat-log on

【Parameter Description】-

【Default Configuration】 Disable only local NAT log recording.

【Command Mode】 Configuration mode

【Default Level】 14

【Usage Guide】 When this command is enabled, only NAT logs will be recorded. When closed, all flow logs are logged.

【Configuration Example]】1: Enable to record only the local NAT log.

```
AC-FS(config)# ip nat-log on
```

【Verification】1: Use the show nat-log status command to check the open status of this function.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.2nat-log data-store

Set the number of days for local log storage

nat-log data-store days

Restore default configuration.

no nat-log data-store

【Parameter Description】

Parameter	Description
days	Log storage days, take the value range: 10~90.

【Default Configuration】 Save 30 days by default

【Command Mode】 Configuration mode

【Default Level】 14

【Usage Guide】According to the disk capacity and query requirements, the number of days for log storage can be adjusted appropriately.

【Configuration Example]】1: Enable local logging.

```
AC-FS(config)# nat-log data-store 60
```

【Verification】1: Use the show run command to view the currently configured days. The default is 30 days.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.3nat-log enable

Enable local logging

nat-log enable

Close nat log.

no nat-log enable

【Parameter Description】-

【Default Configuration】 Disable nat-log function.

【Command Mode】 Configuration mode

【Default Level】 14

【Usage Guide】 If you want to record flow logs locally, you need to execute this command.

【Configuration Example]】1: Enable local logging.

```
AC-FS(config)# nat-log enable
```

【Verification】1: Use the show nat-log status command to check the open status of NAT_LOG.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.4rlog dev-ip

Set RLOG local IP.

rlog dev-ip ip

Unset the RLOG local IP.

no rlog dev-ip

【Parameter Description】

Parameter	Description
ip	The specified RLOG local IP.

【Default Configuration】-

【Command Mode】 Configuration mode

【Default Level】 14

【Usage Guide】Local IP Field is required in some logs, so the device needs to set this value according to the local external IP.

This value is mainly passed to the log server. If it is not configured, the server may parse the information incorrectly.

【Configuration Example】1: Configure the local IP as 10.10.10.2.

```
AC-FS(config)# rlog dev-ip 10.10.10.2
```

【Verification】1: Use the show rlog command to view the value of dev-ip.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.5rlog export-rate

Configure RLOG send rate

rlog export-rate val

Cancel send rate configuration

no rlog export-rate

【Parameter Description】

Parameter	Description
val	The number of logs is sent per second in the value range of 10-100,000.

【Default Configuration】 Send 1000 logs per second.

【Command Mode】 Configuration mode

【Default Level】 14

【Usage Guide】 The sending rate depends on the device performance and the number of logs generated by the device.

If the configuration is too large, the CPU of the device may be too high, and if the configuration is too small, the logs may be lost.

【Configuration Example]】1: Configure the RLOG log sending rate to be 10000 per second.

rlog export-rate 10000

【Verification】1: Use the show rlog command to view the current RLOG log sending rate.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.6rlog filter

Set filter conditions for flow logs and local logs

rlog filter aclid

Cancel the filter conditions for flow logs and local logs

no rlog filter

【Parameter Description】

Parameter	Description
aclid	Specified filter ACL condition, take the value range: 2000-2699.

【Default Configuration】-

【Command Mode】 Configuration mode

【Default Level】 14

【Usage Guide】This configuration takes effect on both flow logs and local logs. Use this configuration when the volume of flow logs is too large or you do not need to record all flow logs.

【Configuration Example]】1: Configure to filter flow logs according to the conditions of ACL 2000.

```
AC-FS(config)# access-list 2000 permit udp any any
AC-FS(config)# rlog filter 2000
```

【Verification】1: Use the show run command to check whether the command is configured.

【Prompt Information】-

【Common Mistake】 The corresponding ACL is not configured.

The configured ACL ID is out of the specified range.

【Platform Description】 -

1.7rlog server

Configure the RLOG server

rlog server ip-address [oob] [port port-num]

Shut down the RLOG server.

no rlog server ip-address

【Parameter Description】

Parameter	Description
Ip-address	Server ip.
port-num	Server terminal.
oob	Oob joggle.

【Default Configuration】-

【Command Mode】 Configuration mode

【Default Level】 14

【Usage Guide】 To send logs to the server, first configure the ip, port and other information of a server.

device information.

This information must be configured and whether oob Parameter and vrf Parameter are accurate.If the configured server already exists, the information for the server is modified.

【Configuration Example]】1: Configure a server with an address of 10.10.10.10 and a port of 20000.

```
AC-FS(config)# rlog server 10.10.10.10 port 20000
```

【Verification】1: Use the show rlog command to check whether the server has taken effect.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.8rlog set

Set RLOG to combine multiple logs into one message

rlog set log-com

Disable log merging.

no rlog set log-com

【Parameter Description】-

【Default Configuration】-

【Command Mode】 Configuration mode

【Default Level】 14

【Usage Guide】Enabling this command can improve the log sending efficiency to a certain extent, but it needs the support of the log server.

If the log server does not support the function of combining multiple logs into the same packet, the logs may be lost or cannot be parsed.

【Configuration Example】-

【Verification】1: Use the show rlog command to check whether this setting is enabled.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.9rlog sn-mac-on

Set flow log to include sn and mac information

rlog sn-mac-on

Unset flow log to include sn and mac info

no rlog sn-mac-on

【Parameter Description】-

【Default Configuration】 Not enabled

【Command Mode】 Configuration mode

【Default Level】 14

【Usage Guide】When this configuration is enabled, the flow log sent to the log server will contain sn and mac information, and the server must be able to parse this information.

This configuration requires pre-confirmation that the server is compatible.

【Configuration Example]】1: Enable the flow log with sn and mac information switch.

```
AC-FS(config)# rlog sn-mac-on
```

【Verification】1: Use the show run command to check whether the command is configured.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.10rlog type

Configure specified types of logs to send or generate files

rlog type n server server-ip priority prio

rlog type n file

Cancel the specified log sending

no rlog type n server server-ip

no rlog type n file

【Parameter Description】

Parameter	Description
n	RLOG log type.
server-ip	Configured server IP.
prio	Log sending priority, the value ranges from 0 to 7. The smaller the value, the higher the priority.

【Default Configuration】-

【Command Mode】 Configure global mode

【Default Level】 14

【Usage Guide】 This configuration is required for sending logs. This command must be configured for each log that needs to be sent. If the log is to be sent as a file, it needs to be used with rlog-file.

【Configuration Example]】1: Configure the flow log to be sent to the server 10.10.10.10.

```
AC-FS(config)# rlog type 16 server 10.10.10.10 priority 1
```

【Verification】1: Use the show rlog-status command to see which logs are currently opened on the server.

【Prompt Information】 1: If the specified RLOG server does not exist, an error will be reported and the configuration will not take effect.

【Platform Description】 -

1.11rlog-file send

Set RLOG file upload Parameter

rlog-file send time-range from from-hour to to-hour

rlog-file send compress { zip | none } rlog-file send format {elog | macc }

Unset the RLOG file upload Parameter.

no rlog-file send time-range no rlog-file send compress no rlog-file send format

【Parameter Description】

Parameter	Description
from-hour	Specifies the start time for the scheduled file upload in a 24-hour system.
to-hour	Specifies the end time of the scheduled file upload, for 24 hours, and can be smaller than the from-hour, Indicates across the sky.

【Default Configuration】 Real-time upload, ftp method, zip compression, key-val format

【Command Mode】 Configuration mode

【Default Level】 14

【Usage Guide】 To upload logs in file mode, you need to configure the parameters for log upload.

This value needs to be agreed with the log server. If it is not configured, the log may not be uploaded normally.

【Configuration Example]】1: Configure to send logs regularly, from 22:00 to 6:00 am.

```
AC-FS(config)# rlog-file send time-range from 22 to 6
2：Configure the upload compression mode is zip Configure the upload
compression mode is zip
AC-FS(config)# rlog-file send compress zip
3：Profile log format in json format AC-FS(config)#
rlog-file send format elog
```

【Verification】1: Use the show rlog-file command to view the value.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.12rlog-file server

Set RLOG file server information

rlog-file server protocal ip-address [port port-num] [oob] [path server-path-string] [username username-string passwd passwd-string]

Unset the RLOG file server.

no rlog-file server

【Parameter Description】

Parameter	Description
protocal	Protocol, FTP, or HTTP.
ip-address	Specified RLOG file server ip address.
port-num	Specifies the RLOG File Server Service port, only for HTTP servers, with the default of 80.
oob	Specifies the oob Parameter, and currently only the HTTP mode is valid.
server-path-string	Server directory, the default directory is '/'.
username-string	User name, the default is AC-FS.
passwd-string	Password, the default is AC-FS.

【Default Configuration】-

【Command Mode】 Configuration mode

【Default Level】 14

【Usage Guide】 When you need to configure file upload, you need to configure a file server.

Currently only one file server is supported, and multiple configurations will overwrite the configured content.

【Configuration Example】1: Configure an FTP server.

```
AC-FS(config)# rlog-file server 10.10.10.2 path rlog/ username test passwd test
```

【Verification】1: Use the show rlog-file command to check whether the server information is consistent.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.13rlog-file type

Set the log type for RLOG file upload

rlog-file type type-num

Unset the RLOG file upload Parameter.

no rlog-file type type-num

【Parameter Description】

Parameter	Description
type-num	Log type

【Default Configuration】-

【Command Mode】 Configuration mode

【Default Level】 14

【Usage Guide】 Set this value when you need to enable log file upload.

If this command is not enabled, the log will not be uploaded.

【Configuration Example]】1: Configure to send URL audit logs as files.

```
AC-FS(config)# rlog-file type 20
```

【Verification】1: Use the show rlog command to view the value.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.14 show nat-log

View local log information

Show nat-log [username user_name] [ip-protocol ip-protocol] [source-ip source-ip] [dst-ip dst-ip] [src-port src-port] [dst-port dst-port] time- interval begin-year begin-mon begin-day begin-hour to end-year end-mon end-day end-hour

【Parameter Description】

Parameter	Description
user_name	user name .
ip-protocol	Agreement number.
source-ip	source ip.
dst-ip	purpose,ip.
src-port	Source port, value range: 0-65535.
dst-port	Target port, take the value range: 0-65535.
begin-year	Start time year, value range: 1993-2035.
begin-mon	Start time month, take the value range: 1-12.
begin-day	Start time date, take the value range: 1-31.
begin-hour	Start time hour, take the value range: 0-23.
end-year	End time year, Value range: 1993-2035.
end-mon	End time month, take the value range: 1-12.
end-day	End time date, take the value range: 1-31.
end-hour	End time hour, take the value range: 0-23.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 This command is used to query the flow/NAT logs recorded in a period of time, which can be filtered according to user name, protocol number, source ip, destination ip, source port, and destination port.

【Configuration Example]】1: The following example looks at the log records from 3:00 to 5:00 on October 6, 2010.

```
AC-FS#show nat-log time-interval 2010 10 6 3 t 2010 10 6 5
count:427
Pr  SrcAddr                         DstAddr                         UserName
SrcPort       DstPort       Vrf       SendBytes  RecvBytes  time
17  192.168.122.62 (0.0.0.0)        192.168.122.255(0.0.0.0)        192.168.122.62
138  (0)      138  (0)      0         2028       0          2010-10-6 3:1
17  192.168.100.55 (0.0.0.0)        192.168.100.255(0.0.0.0)        192.168.100.55
138  (0)      138  (0)      0         732        0          2010-10-6 3:1
17  192.168.122.54 (0.0.0.0)        192.168.122.255(0.0.0.0)        192.168.122.54
137  (0)      137  (0)      0         864        0          2010-10-6 3:1
138  (0)      138  (0)      0         714        0          2010-10-6 3:3
```

Field Description:

Field	Description
Pr	protocol
SrcAddr	source address
DstAddr	destination address
UserName	user name
SrcPort	source port
DstPort	destination port
Vrf	VRF name
RecvBytes	Receive the number of bytes
time	Flow time

【Prompt Information】-

【Platform Description】 -

1.15 show rlog

View RLOG configuration information

show rlog

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to view the RLOG server, local device IP, sending rate, send log statistics, log merge function, etc.

【Configuration Example]】1: View RLOG configuration information.

```
AC-FS#show    rlog
rlog server is enable
 port 20000  server 192.168.1.100
 port 20000 server 10.10.10.10
rlog dev-ip 0.0.0.0
rlog export-rate 1000 rlog queue remain 10000
send log count : 0 error count : 0 errorno : 0
recv buf: 0 poll buf err: 0 push buf: 0 local buf: 0
recv err cnt: 0 depatch err cnt: 0

enable log combination: 0
```

Field Description:

Field	Description
rlog server is enable	The server is configured, the following N behavior for specific server ports and IP.
rlog dev-ip	Device local IP.
rlog export-rate	Log send rate.
rlog queue remain	Number of remaining nodes in the log cache.
send log count	Number of logs sent.
error count	Number of failed logs.
errorno	Last send a failed error code.
recv buf	Number of logs received by the RLOG.
poll buf err	Number of times with insufficient log cache space.
local buf	Number of local log output.
recv err cnt	The number of errors that you received the message.
depatch err cnt	Received a message that does not have a corresponding server, or the server for the message is invalid.

enable log combination	Whether to do the log merge to send.

【Prompt Information】 If no server is configured, this command does not display anything.

【Platform Description】 -

1.16 show rlog-file

View the configuration information of the RLOG file mode

show rlog-file

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to view the server information of the RLOG file, the log storage path, the size of the log directory, the log sending type and sending Parameter, etc.

【Configuration Example]】1: View RLOG configuration information.

```
AC-FS#show rlog-file
rlog file server ftp:
     ip:10.10.10.2, port:21 oob
     path: rlog/
     username:ftp passwd:ftp
local path: /tmp/rlog-file
local storage: 65536 K
send time-rage: from 22 to 6
send compress: zip; format: json
total proc files: 99
client count: 2
log          total tar|err  send|err  lasterr
LOG          100    100|0    100|0     0
MAIL_BODY    100    100|0    100|0     0
MAIL_ATTACH   100   100|0      100|0      0
WEBMAIL     100     100|0     100|0       0
BSS_BODY 100  100|0  100|0  0

send log type:
RLOG_FILE_TYPE_URL_AUDIT  20
```

Field Description:

Field	Description
ip	server IP.
port	Server terminal.
oob	Send it through the management port.
path	The Server uploads the directory.
username	Server username.
passwd	Server password.
local path	Local storage path.
local storage	Local storage size upper limit.
send time-rage	Regular transmission time range.
send protocal	Log Send Protocol.
total proc files	Number of log files processed.

client count	Number of clients.
tar file error	Number of packaged file errors and the last error code.
put file error	Number of uploaded file errors and the last error code.
send log type	Send log type.

【Prompt Information】-

【Platform Description】 -

1.17 show rlog-status

View RLOG server status.

show rlog-status { [server ip] | [client] | [log] }

【Parameter Description】

Parameter	Description
Ip	Specifies the IP for the specific server.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to view the RLOG server status.

【Configuration Example]】1: View all RLOG server information.

```
AC-FS#show rlog-status
============================================================
server:192.168.1.100       port:20000
type                            prio
============================================================
server:10.10.10.10       port:20000
type                            prio
RLOG_TYPE_FLOW        16         1
```

Field Description:

Field	Description
server	Server address.
port	Server terminal.
type	Log Types for Server Provisioning.
prio	Log priority for the server opening.

2: View the number of function modules connected to RLOG.

```
AC-FS#show rlog-status client

rlog client count: 0
```

Field Description:

Field	Description
rlog client count	Number of RLOG functional modules received.

3: View the number of logs received by RLOG

```
AC-FS#show rlog-status log

local rlog message:


remote rlog message:

[16]RLOG_TYPE_FLOW                : 0

[17]RLOG_TYPE_CPU_MEM             : 0
```

```
[18]RLOG_TYPE_DISC          :          0
[19]RLOG_TYPE_DEV_LOG       :          0
[20]RLOG_TYPE_URL_AUDIT     :          0
[21]RLOG_TYPE_SESSION       :          0
[22]RLOG_TYPE_IP_APP        :          0
[23]RLOG_TYPE_IP            :          0
[24]RLOG_TYPE_CHANNEL       :          0
[25]RLOG_TYPE_INTERFACE     :          0
[26]RLOG_TYPE_IP_OFFLINE    :          0
[27]RLOG_TYPE_MAIL_AUDIT    :          0
[28]RLOG_TYPE_TELNET_AUDIT  :          0
[29]RLOG_TYPE_WEB_SEARCH_AUDIT    : 0
[30]RLOG_TYPE_WEB_BBS_AUDIT  :         0
[31]RLOG_TYPE_IM_AUDIT      :          0
[32]RLOG_TYPE_FTP_AUDIT     :          0
[33]RLOG_TYPE_WEB_AUDIT     :          0
[34]RLOG_TYPE_APP_AUDIT     :          0
[35]RLOG_TYPE_FLOOD         :          0
[36]RLOG_TYPE_FLOOD_CEASEm  :          0
[37]RLOG_TYPE_SCAN          :          0
[38]RLOG_TYPE_SCAN_CEASE          : 0
[39]RLOG_TYPE_ATTACK_FRAG         : 0
```

Field Description:

Field	Instruction
local rlog message	The RLOG local log number information is received.
remote rlog message	Number of RLOG remote logs received, by log type area component.

【Prompt Information】 1: If there is no server configured on the device, this command will not display anything.

【Platform Description】 -

1.18 show rlog-type

Check what log types RLOG has.

show rlog-type

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to check the log types of RLOG.

【Configuration Example]】1: View RLOG log types.

```
AC-FS#show rlog-type
RLOG_TYPE_FLOW                16
RLOG_TYPE_CPU_MEM             17
RLOG_TYPE_DISC                18
RLOG_TYPE_DEV_LOG             19
RLOG_TYPE_URL_AUDIT           20
RLOG_TYPE_SESSION             21
RLOG_TYPE_IP_APP              22
RLOG_TYPE_IP                  23
RLOG_TYPE_CHANNEL             24
RLOG_TYPE_INTERFACE           25
RLOG_TYPE_IP_OFFLINE          26
RLOG_TYPE_MAIL_AUDIT          27
RLOG_TYPE_TELNET_AUDIT        28
RLOG_TYPE_WEB_SEARCH_AUDIT    29
RLOG_TYPE_WEB_BBS_AUDIT       30
RLOG_TYPE_IM_AUDIT            31
RLOG_TYPE_FTP_AUDIT           32
RLOG_TYPE_WEB_AUDIT           33
```

```
RLOG_TYPE_APP_AUDIT              34
RLOG_TYPE_FLOOD                  35
RLOG_TYPE_FLOOD_CEASEm           36
RLOG_TYPE_SCAN                   37
RLOG_TYPE_SCAN_CEASE             38
RLOG_TYPE_ATTACK_FRAG            39
```

Field Description:

Field	Description
-	Format is the log type name, and the log type takes the value.

【Prompt Information】 1: If there is no server configured on the device, this command will not display anything.

【Platform Description】 -

10 POLICE-LOG

10.1 content-audit write-plog

Enable content audit network monitor log.

[no] content-audit write-plog {im | mail | url | vid | web-bbs | web-mail | web-search}

Close the content audit network monitor log.

[no] content-audit write-plog {im | mail | url | vid | web-bbs | web-mail | web-search}

【Parameter Description】

Parameter	Description
im	Open the im chat log to send the network supervisor.
mail	Open the client mail log sending network supervisor.
url	Open the http log to send the network supervisor.
vid	Open the virtual identity audit to send the network supervisor.
web-bbs	Open the forum log to send the network supervisor.
web-mail	Open the web-terminal mail log sending network supervisor.
web-search	Open the search log to send the network supervisor.

【Default Configuration】 The default is the closed state.

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 This command enables the user to enable the content audit log sending network monitoring module

【Configuration Example]】1: Enable content audit log sending to network monitor

```
AC-FS(config)#content-audit write-plog ?
  im          Im audit information
  mail        Mail audit information
  url         Url audit information
  vid         Vid audit information
  web-bbs     Web-bbs audit information
  web-mail    Web-mail audit information
  web-search  Web-search audit information
```

```
AC-FS(config)#content-audit write-plog
```

【Verification】Use the show content-audit plog config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

10.2 debug police-log

Enable debug logging at the specified log level.

debug police-log {auth | common | mail | nat | setdev | url | vid | webbbs | websearch}

Default log level

no debug police-log {auth | common | mail | nat | setdev | url | vid | webbbs | websearch}

or

undebug police-log {auth | common | mail | nat | setdev | url | vid | webbbs | websearch}

【Parameter Description】

Parameter	Description
-auth	Open the authentication log debug information.
-common	Turn on the 5 content audit log debug information.
-getdev	Open the premises information for debug information.

-mail	Open the mail log debug information.
-nat	Open the nat log debug information.
-setdev	Turn on for the heartbeat debug information.
-url	Turn on the http log debug information.
-vid	Open the virtual identity log debug information.
-webbbs	Open the forum log debug information.
-websearch	Open the search log debug information.

【Default Configuration】 None

【Command Mode】 Privileged mode

【Default Level】15

【Usage Guide】 This command is a debugging switch, which is used for troubleshooting. For example, the MACC display device is offline. At this time, you can open the log and view the detailed information of the interaction between the network monitoring module and the MACC.

The debug log of this module is output using the rg_syslog module, and the log on and log console commands need to be enabled.

【Configuration Example】1: Enable debug log.

```
AC-FS#debug police-log ?
  auth       Open auth police log debug
  common     Open all common police log debug
  getdev     Open get dev status debug
  mail       Open mail police log debug
  nat        Open nat police log debug
  setdev     Open set dev status debug
  url        Open url police log debug
  vid        Open vid police log debug
  webbbs     Open webbbs police log debug
  websearch  Open websearch police log debug
```

2: Turn off debug logging.

```
AC-FS#no debug police-log ?
  auth        Open auth police log debug
  common      Open all common police log debug
  getdev      Open get dev status debug
  mail        Open mail police log debug
  nat         Open nat police log debug
  setdev      Open set dev status debug
  url         Open url police log debug
  vid         Open vid police log debug
  webbbs      Open webbbs police log debug
  websearch   Open websearch police log debug
```

【Debug information】 1: Request location information from MACC.

Debug information	https://192.168.23.206/specification/service/dc/getDevConf post data:{"device_sn":"1234842571023", "device_mac":"00-D0-F8-22-35-35", "device_type":0}
Information interpretation	The device requests site information from the MACC.
cause	Device boot, and interval update site information trigger.
Deal with suggestions	-

2: MACC heartbeat request.

Debug information	https://192.168.23.206/specification/service/ds/setDevStatus post data:{"netbar_wacode":"35011110341520","collection_equipment_id": "75496176400D0F8223535", "device_status":"00"} {"code":0,"msg":"ok"}
Information interpretation	The device sends the heartbeat request package to the MACC, and the MACC returns the heartbeat successfully.
cause	Time ed heartbeat with the MACC .
Deal with suggestions	-

3. Report log files to MACC.

Debug information	https://120.35.11.138:4433/specification/service/fileUpload?collection_equipment_id= 754961764FFFFFFFFFFF&line_count=31 /tmp/log//145-010000-1456709687-00000-WA_SOURCE_FJ_0001-0.xml {"code":"0","msg":"ok"}

Information interpretation	Send log file to MACC, MACC returns successful reception.
cause	The log of the premises on the device needs to be uploaded to the MACC
Deal with suggestions	-

【Verification】 Use the show debuging command to view the configuration status.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

10.3 nat-log police

Enable NAT flow log auditing.

nat-log police

Turn off NAT flow log auditing.

no nat-log police

【Parameter Description】 -

【Default Configuration】 The default is the closed state.

【Command Mode】 Global mode

【Default Level】 15

【Usage Guide】 This command enables the user to enable monitoring of NAT flow logs.

【Configuration Example】 1: Enable network monitoring module.

```
AC-FS# configure AC-FS(config)#
nat-log police AC-FS(config)#
exit
AC-FS# wr
```

【Verification】Use the show nat-log status command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

10.4police-log enable

Enable police-log.

police-log enable

Disable police-log.

no police-log enable

【Parameter Description】-

【Default Configuration】 The default is the closed state.

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 This command enables the user to start the network monitoring program, connect with the MACC, and send the corresponding logs.

【Configuration Example】1: Enable network monitoring module.

```
AC-FS#   configure AC-FS(config)#
police-log enable AC-FS(config)#
exit
AC-FS# wr
```

【Verification】Use the show police-log config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

10.5police-log file-sender compress

Enable police-log compressed log function.

police-log file-sender compress

Disable the police-log compressed log function.

no police-log file-sender compress

【Parameter Description】-

【Default Configuration】 The default is the closed state.

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 This command is used to compress or uncompress the log of sending MACC/ELOG.

【Configuration Example]】1: Enable network monitor log compression.

```
AC-FS#config
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)#police-log  file-sender  compress AC-FS(config)#
AC-FS# wr
```

【Verification】Use the show police-log config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

10.6police-log set url

Set MACC/ELOG docking address

police-log set url url

Clear MACC/ELOG docking address

no police-log set url

【Parameter Description】

Parameter	Description
url	MACC/ELOG Full URL access home page, note if MACC/ELOG is in a subdirectory of a server.

【Default Configuration】The address is empty

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 This command is used to configure the url of the MACC/ELOG server. Please note that it is the complete MACC/ELOG service host address. Some hosts will deploy multiple sets of WEB services

【Configuration Example]】1: Configure the interconnection address of MACC to https://172.18.124.35/specification/.

```
AC-FS# configure
AC-FS(config)# police-log set url https://172.18.124.35/specification/ AC-
FS(config)# exit
AC-FS# wr
```

【Verification】Use the show police-log config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

10.7 show police-log config

Display the configuration information of the network monitor component

show police-log config

【Parameter Description】-

【Command Mode】 Privileged mode, global mode

【Usage Guide】 It is used to check the operation of the network monitoring module, whether it is enabled, whether it is successfully connected with the MACC, etc.

【Configuration Example]】1: View network monitoring module configuration information.

```
AC-FS#show police-log config
police log configuration
    >police log: enable
    >server url: https://192.168.25.184:443/specification
```

```
    >auth type: define (1021999)
    >file compress: enable
```

Field Description:

Field	Description
police-log	Whether the network monitoring module is on, enable means on and disable means close.
server url	MACC / ELOG Server address.
auth type	Certification type configuration.
file compress	File compression switch: enable compression, disable compression.

【Prompt Information】-

【Platform Description】 -

10.8 show police-log status

Display the running status of the network monitor component

show police-log status

【Parameter Description】-

【Command Mode】 Privileged mode, global mode

【Usage Guide】 It is used to check the operation of the network monitoring module, whether it is enabled, whether it is successfully connected with the MACC, etc.

【Configuration Example]】1: View the running status of the network monitoring module.

```
AC-FS#show police-log status

>police-log:     enable
>server status:  connected
>log total deal: 2626   speed:0
>file total send:184    failed:16       waitting:0
>compress:       disable

in>  rcv:2,   deal:2,  fail:0
out>  rcv:2,  deal:2,  fail:0
```

```
file> send:1,     fail:3,          drop:1

in>     rcv:2568,  deal:2568,          fail:0
out>    rcv:2568,  deal:2568,          fail:0
file> send:141,   fail:50,   drop:13

in>    rcv(vid):0,         deal:0,   fail:0
out>   rcv(vid+im):19,    deal:19,          fail:0
file> send:15,    fail:5,          drop:1

out>   rcv:37,    deal:37,          fail:0
file> send:11,    fail:7,          drop:1

out>   rcv:0,     deal:0,   fail:0
file> send:0,     fail:0,          drop:0

out>   rcv:0,     deal:0,   fail:0
file> send:0,     fail:0,          drop:0

out>   rcv:0,     deal:0,   fail:0
file> send:0,     fail:0,          drop:0
```

Field Description:

Field	Description
police-log	Whether the network monitoring module is enabled, enable means open, disable means close.
server status	Whether the communication of MACC is connected, connected means connected, disconect means not connected.
log total deal	The total number and speed of processing logs.
file total send	The total number of log files sent and the number of failures.
compress	File compression switch: enable compression, disable no compression.
AUTH LOG	Authentication log statistics.
NAT LOG	nat log statistics.
VID LOG	Virtual identity log statistics.
URL LOG	http log statistics.

MAIL LOG	Mail log statistics.
WEBBBS LOG	bbs forum log statistics
WEBSEARCH LOG	Search log statistics

【Prompt Information】-

【Platform Description】 -

11 CWMP

11.1acs password

Configure the password used for authentication when the CPE connects to the ACS.

acs password {password | encryption-type encrypted-password}

Restore Default Configuration

no acs password

【Parameter Description】

Parameter	Description
password	CPE connects the ACS for authentication.
encryption-type	It can be configured as 0 or 7, and 0 means no encryption, and 7 means simple encryption.
encrypted-password	cryptogram.

【Default Configuration】 The default encryption-type is 0, and the encrypted-password is empty by default.

【Command Mode】 cwmp configuration mode

【Default Level】1

【Usage Guide】 Configure the password used by CPE to connect to ACS for authentication. Usually, you do not need to enter the encryption type. In general, the encryption type is only required when copying and pasting the encrypted password for the command. The format requirements for a valid password are as follows:

1. Password must be English letters or numbers.

2. Spaces in the middle and at the end of the password are part of the password.

【Configuration Example]】1: Configure the password used for authentication when the CPE connects to the ACS as "123".

```
AC-FS#config
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)#cwmp
AC-FS(config-cwmp)#acs password 123
AC-FS(config-cwmp)#
```

【Verification】Run the show cwmp configuration command on the CPE device to check whether the command is configured successfully.

【Prompt Information】 1: If the user enters the password type as cipher text, the length of the password exceeds 254 or the length is not an even number, it will prompt an error.

%%Error: Invalid Encrypted Password

2: If the password type entered by the user is plain text and the password length exceeds 100, an error will be prompted.

%%Error: The Length of ACS's Password is Too Long

3: If the password type entered by the user is plaintext and contains illegal characters, an error will be prompted

%%Error: Password String Include Invalid Characters!

【Common Mistake】 1. If the password type entered by the user is cipher text, the length of the password exceeds 254 or the length is not an even number.

2. If the user input password type is clear text, the password length exceeds 100.

3. If the user input password type is clear text and contains illegal characters.

【Platform Description】 -

11.2acs url

Configure the URL for the CPE to connect to the ACS.

acs url url

Restore Default Configuration.

no acs url

【Parameter Description】

Parameter	Description
url	URL of ACS.

【Default Configuration】-

【Command Mode】 cwmp configuration mode

【Default Level】1

【**Usage Guide**】Configure the URL for CPE to connect to the ACS. Without manually configuring the ACS URL, if a dynamic ACS URL is obtained using DHCP, the dynamically obtained ACS URL will be used to initiate a connection to the ACS. The URL format requirements for ACS are as follows:

1. The URL format of the ACS must be in the format: http://host[:port]/path (or https://host[:port]/path).

2. The maximum length of the ACS URL is 256 characters.

【**Configuration Example]**】1: Configure the URL for CPE to connect to the ACS as "http://10.10.10.1:8080/acs".

```
AC-FS#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)#cwmp
AC-FS(config-cwmp)#acs url http://10.10.10.1:8080/acs
AC-FS(config-cwmp)#
```

2: Configure the URL of the CPE to connect to the ACS as "http://www.test.com/service/tr069servlet".

```
AC-FS#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)#cwmp
AC-FS(config-cwmp)#acs url http://www.test.com/service/tr069servlet
AC-FS(config-cwmp)#
```

【**Verification**】Run the show cwmp configuration command on the CPE device to check whether the command is configured successfully.

【**Prompt Information**】 1: If the ACS URL address is NULL, it will prompt an error.

```
input acs attribute parameter is null
```

【**Common Mistake**】 1. The ACS URL is not entered in the required format.

2. ACS URL is longer than 256 characters.

【**Platform Description**】 -

11.3acs username

Configure the user name used for authentication when the CPE connects to the ACS.

acs username username

Restore Default Configuration.

no acs username

【**Parameter Description**】

Parameter	Description
- username	The user name used by CPE to connect ACS for authentication.

【Default Configuration】 is empty.

【Command Mode】 cwmp configuration mode

【Default Level】1

【Usage Guide】 Configure the user name used for authentication when the CPE connects to the ACS.

【Configuration Example]】1: Configure the user name for authentication when CPE connects to ACS is "admin"

```
AC-FS#config
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)#cwmp
AC-FS(config-cwmp)#acs username admin
AC-FS(config-cwmp)#
```

【Verification】Run the show cwmp configuration command on the CPE device to check whether the command is configured successfully.

【Prompt Information】 1: If the user input user name is NULL, it will prompt an error.

```
input acs attribute parameter is null
```

【Common Mistake】-

【Platform Description】 -

11.4 cpe back-up

Configure the CPE main program/configure the backup and restore function. cpe back-up [delay-time seconds] Close the main program of CPE/configuration backup and restore function no cpe back-up

【Parameter Description】

Parameter	Description
seconds	CPE master / configuration backup Restore delay time, in seconds, with values ranging from 30 to 10,000.

【Default Configuration】 The default value is 60 seconds.

【Command Mode】 cwmp configuration mode

【Default Level】1

【Usage Guide】Configure the recovery function of the CPE main program/configuration in abnormal situations, which means that when the CPE cannot connect to the ACS after the main program/configuration upgrade, and the disconnection occurs, the main program and configuration before the disconnection can be recovered in time. Configure and restore the management of the CPE by the ACS. This situation is generally caused by the wrong main program or configuration being issued.

【Configuration Example]】1: Disable the CPE main program/configuration backup and restore function.

```
AC-FS#config
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)#cwmp
AC-FS(config-cwmp)#no cpe back-up
AC-FS(config-cwmp)#
```

【Verification】Run the show cwmp configuration command on the CPE device to check whether the command is configured successfully.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

11.5 cpe inform

Configure the periodic INFORM notification function of the CPE.

cpe inform [interval seconds] [starttime time]

Restore Default Configuration.

no cpe inform

【Parameter Description】

Parameter	Description

seconds	Configure the CPE periodic INFORM notification time interval.In seconds, the values range from 30 to 3600.
time	Date time of starting periodic INFORM in yyyy-mm-ddThh: mm: ss.

【Default Configuration】 The default value is 600 seconds.

【Command Mode】 cwmp configuration mode

【Default Level】1

【Usage Guide】 Configure the periodic INFORM notification function of CPE.

1. If the INFORM start time is not configured, the periodic INFORM starts from this function, and announces it every time an INFORM cycle passes.

2. When the INFORM start date time is configured, the start time of the periodic INFORM is the specified time. If the INFORM period is configured to be 60 seconds and the start time is 12:00 noon tomorrow, the periodic INFORM announcement will not start until 12:00 noon tomorrow, and the INFORM announcement will be made every 60 seconds.

The shorter the periodic INFORM notification interval of the CPE, the more timely the ACS can track the latest status of the CPE, and the more frequent the sessions between the CPE and the ACS, the more resources of the CPE and the ACS are consumed. and the performance of the ACS configure the appropriate interval.

【Configuration Example]】1: Configure the CPE cycle INFORM notification interval to 60 seconds.

```
AC-FS#config
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)#cwmp
AC-FS(config-cwmp)#cpe inform interval 60
AC-FS(config-cwmp)#
```

【Verification】Run the show cwmp configuration command on the CPE device to check whether the command is configured successfully.

【Prompt Information】-

【Common Mistake】 None.

【Platform Description】 -

11.6 cpe password

Configure the password used for authentication when the ACS connects to the CPE. The no form of this command restores the Default

Configuration.

cpe password {password | encryption-type encrypted-password}

Restore Default Configuration.

no cpe password

【Parameter Description】

Parameter	Description
password	Password for the ACS connection CPE for authentication.
encryption-type	It can be configured as 0 or 7, and 0 means no encryption, and 7 means simple encryption.
encrypted-password	Password text.

【Default Configuration】 The default encryption-type is 0, and the encrypted-password is empty by default.

【Command Mode】 cwmp configuration mode

【Default Level】1

【Usage Guide】 Configure the password used by the ACS to connect to the CPE for authentication. Usually, you do not need to enter the encryption type. In general, the encryption type is only required when copying and pasting the encrypted password for the command. The format requirements for a valid password are as follows:

1. Consists of English letters and numbers.

2. The password can be preceded by leading spaces, but ignored. Intermediate and trailing spaces are part of the password.

【Configuration Example]】1: Configure the password used for authentication when the ACS connects to the CPE as "123".

```
AC-FS#config
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)#cwmp
AC-FS(config-cwmp)#cpe password 123
AC-FS(config-cwmp)#
```

【Verification】Run the show cwmp configuration command on the CPE device to check whether the command is configured successfully.

【Prompt Information】 1: If the user enters the password type as cipher text, the length of the password exceeds 254 or the length is not an even number, it will prompt an error.

```
%%Error: Invalid Encrypted Password
```

2: If the password type entered by the user is plain text and the password length exceeds 100, an error will be prompted.

%%Error: The Length of ACS's Password is Too Long

3: If the password type entered by the user is plaintext and contains illegal characters, an error will be prompted

%%Error: Password String Include Invalid Characters!

4: If the password type entered by the user is cipher text and contains illegal characters (legal characters can only be: numbers 0~9, characters a~f, A~F), an error will be prompted.

%%Error: Invalid Encrypted Password

【Common Mistake】 1. If the password type entered by the user is cipher text, the length of the password exceeds 254 or the length is not an even number.

2. If the user input password type is clear text, the password length exceeds 100.

3. If the user input password type is clear text and contains illegal characters.

4. If the user input password type is cipher text and contains illegal characters (legal characters can only be: numbers 0~9, characters a~f, A~F).

【Platform Description】 -

11.7 cpe url

Configure the URL for the ACS to connect to the CPE.

cpe url url

Restore Default Configuration.

no cpe url

【Parameter Description】

Parameter	Description
url	The URL of the CPE.

【Command Mode】 cwmp configuration mode

【Default Configuration】-

【Default Level】1

【Usage Guide】Configure the URL of the ACS to connect to the CPE. If there is no manual configuration, the CPE will automatically select the URL of the CPE according to the URL of the ACS. The URL format of the CPE is as follows:

1. The URL of the CPE must be in the format http://ip [: port]/".

2. The maximum length of the CPE URL is 256 characters.

【Configuration Example]】1: Configure the URL of the ACS to connect to the CPE as "http://10.10.10.1:7547/".

```
AC-FS#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)#cwmp
AC-FS(config-cwmp)#cpe url http://10.10.10.1:7547/
AC-FS(config-cwmp)#
```

【Verification】Run the show cwmp configuration command on the CPE device to check whether the command is configured successfully.

【Prompt Information】 1: If the URL address of the CPE is NULL, it will prompt an error.

```
input CPE attribute parameter is null
```

【Common Mistake】 1. The CPE URL is not entered in the required format.

2. The CPE URL is longer than 256 characters.

【Platform Description】 -

11.8 cpe username

Configure the user name used for authentication when the ACS connects to the CPE.

cpe username username

Restore Default Configuration.

no cpe username

【Parameter Description】

Parameter	Description
username	Configure the user name that the ACS connection CPE uses for authentication.

【Command Mode】 cwmp configuration mode

【Default Configuration】-

【Default Level】1

【Usage Guide】 Configure the user name used for authentication when the ACS connects to the CPE.

【Configuration Example]】1: Configure the user name for authentication when the ACS connects to the CPE is "admin"

```
AC-FS#config
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)#cwmp
AC-FS(config-cwmp)#cpe username admin
AC-FS(config-cwmp)#
```

【Verification】Run the show cwmp configuration command on the CPE device to check whether the command is configured successfully.

【Prompt Information】 1: If the user input user name is NULL, it will prompt an error.

```
input acs attribute parameter is null
```

【Common Mistake】-

【Platform Description】 -

11.9cwmp

Configure to enable/disable CWMP function.

cwmp

Turn off the CWMP function.

no cwmp

【Parameter Description】-

【Command Mode】 Global configuration mode

【Default Level】1

【Usage Guide】 Configure the function status of CWMP.

【Configuration Example】1: Disable the CWMP function.

```
AC-FS#config
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)#no cwmp
AC-FS(config)#
```

【Verification】Run the show cwmp configuration command on the CPE device to check whether the command is configured successfully.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

11.10 disable download

The configuration turns off the ability to download the main program and configuration files from the ACS.

disable download

Restore Default Configuration.

no disable download

【Parameter Description】-

【Command Mode】 cwmp configuration mode

【Default Level】1

【Default Configuration】 The CPE file download function is enabled (no disable download).

【Usage Guide】 Configure to disable the function of downloading the main program and configuration files from ACS.

1. This command has no effect on the configuration script file. If disable is configured, the configuration script can be executed.

【Configuration Example]】1: The configuration disables the function of downloading the main program and configuration files from the

ACS.

```
AC-FS#config
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)#cwmp
AC-FS(config-cwmp)#disable download
AC-FS(config-cwmp)#
```

【Verification】Run the show cwmp configuration command on the CPE device to check whether the command is configured successfully.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

11.11 disable upload

The configuration turns off the ability to upload configuration files and log files to ACS.

disable upload

Restore Default Configuration.

no disable upload

【Parameter Description】-

【Command Mode】 cwmp configuration mode

【Default Configuration】 The CPE file upload function is enabled (no disable upload).

【Default Level】1

【Usage Guide】 Configure to disable the function of uploading configuration files and log files to ACS

【Configuration Example]】1: Disable the function of uploading configuration files and log files to ACS.

```
AC-FS#config
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)#cwmp
AC-FS(config-cwmp)#disable upload
AC-FS(config-cwmp)#
```

【Verification】Run the show cwmp configuration command on the CPE device to check whether the command is configured successfully.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

11.12 show cwmp configuration

Displays the current configuration of the CWMP function.

show cwmp configuration

【Parameter Description】

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】

【Configuration Example】1: Display the current configuration of the CWMP function.

```
AC-FS(config-cwmp)#show cwmp configuration
CWMP Status                    : enable
ACS URL                        : http://www.AC-FS.com.cn/acs
ACS username                   : admin
ACS password                   : ******
CPE URL                        : http://10.10.10.2:7547/
CPE username                   : AC-FS
CPE password                   : ******
CPE inform status              : disable
CPE inform interval            : 60s
```

```
CPE inform start time           : 0:0:0 0 0 0
CPE wait timeout                : 50s
CPE download status              : enable
CPE upload status                : enable
CPE back up status  : enable
CPE back up delay time          : 60s
```

Field Description:

Field	Description
CWMP Status	Enabling status of the CWMP function.
ACS URL	The CPE connects to the URL of the ACS.
ACS username	User name of the CPE connection to the ACS.
ACS password	Password for the CPE connection to the ACS.
CPE URL	The ACS connects to the URL of the CPE.
CPE username	Username of the ACS connection to the CPE.
CPE password	Password for the ACS connection to the CPE.
CPE inform status	Periodic INFORM notification status of the CPE.
CPE inform interval	The CPE periodic INFORM notification time interval.
CPE wait timeout	The CPE session timeout time.
CPE inform start time	The CPE periodic INFORM start notification date time.
CPE download status	Do you accept the downloading of the master programs and configuration files from the ACS.
CPE upload status	Whether to upload the profile and log files to the ACS.
CPE back up status	Open the functional status of the master program / configuration Restore.
CPE back up delay time	Wait delay time for the main program / configuration Restore.

【Prompt Information】-

【Platform Description】 -

11.13 show cwmp status

Displays the current operating status of CWMP

show cwmp status

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】1

【Usage Guide】-

【Configuration Example】1: Display the current running status of CWMP.

```
AC-FS(config-cwmp)#show  cwmp  status
CWMP Status                    : enable
Session status                 : Close
Last success session           : Unknown
Last success session time      : Thu Jan 1 00:00:00 1970
Last fail session              : Unknown
Last fail session time         : Thu Jan  1 00:00:00 1970
Session retry times            : 0
```

Field Description:

Field	Description
CWMP Status	Enable state of the CWMP function.
Session status	The current session state between the CPE and the ACS.
Last success session	The type of the last successful session.
Last success session time	Last successful session end time
Last fail session	Type of last failed session.
Last fail session time	Last failed session end time.
Session retry times	The number of retries for the current session.

【Prompt Information】-

【Platform Description】 -

11.14timer cpe-timeout

Configure the ACS unresponsive CPE timeout period.

timer cpe- timeout seconds

Restore Default Configuration.

no timer cpe-timeout

【Parameter Description】

Parameter	Description
seconds	Timeout time. In seconds, the value range from 5 to 600.

【Command Mode】 cwmp configuration mode.

【Default Configuration】 The default value is 5 seconds.

【Default Level】1

【Usage Guide】 Configure the ACS unresponsive CPE timeout period.

1. The maximum delay for the session to wait when the response from the ACS cannot be received due to some abnormal conditions (such as network disconnection)

【Configuration Example]】1: Configure the ACS unresponsive CPE timeout to 50 seconds.

```
AC-FS#config
Enter configuration commands, one per line. End with CNTL/Z.
AC-FS(config)#cwmp
AC-FS(config-cwmp)#timer cpe-timeout 50
AC-FS(config-cwmp)#
```

【Verification】Run the show cwmp configuration command on the CPE device to check whether the command is configured successfully.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

12 LEDs

12.1led on

Turn on the AP locator light

led on [slot slot-id [secondary]]

Turn off the AP location light

no led on [slot slot-id [secondary]]

【Parameter Description】

Parameter	Description
slot-id	The slot position number corresponding to the RF card.
secondary	Cascade devices under the current slot position.

【Default Configuration】 The default is off

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 This command is used to turn on the AP locating light, so as to locate the location of the AP. For rack AP devices, you need to use the command with slot Parameter to turn on the positioning light of each radio card. For non-rack devices, the specified slot Parameter command is invalid. secondary means that it takes effect on the second-level device in the cascade scenario, and it takes effect on the first-level device in the non-cascading scenario or the cascading scenario without the secondary parameter.

【Configuration Example】1: Turn on the AP positioning light.

```
AC-FS(config)#ap-config 00d0.f822.33bc
AC-FS(config-ap)#led on
```

2: Turn off the AP location light.

```
AC-FS(config)#ap-config 00d0.f822.33bc
AC-FS(config-ap)#no led on
```

【Verification】Observe whether the AP positioning LED light is effective.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

12.2quiet-mode session

Configure the LED light in silent mode.

quiet-mode session session-num

Quiet mode with LED off.

no quiet-mode session session-num

【Parameter Description】

Parameter	Description
session-num	Session id.

【Default Configuration】 The default is off

【Command Mode】 AP configuration mode

【Default Level】 14

【Usage Guide】 Configure this command to turn off all the LED lights on the AP

【Configuration Example】1: Configure the LED to be silent from 23:00 to 7:00 the next day

```
AC-FS(config)#schedule session 1
AC-FS(config)#schedule session 1 time-range 1 period Mon time 23:00 to 7:00
AC-FS(config)#ap-config 00d0.f822.33bc
AC-FS(config-ap)#quiet-mode session 1
```

2: Turn off the silent mode of the LED.

```
AC-FS(config)#ap-config 00d0.f822.33bc
AC-FS(config-ap)#no quiet-mode session 1
```

【Verification】During the time period configured by the system time, all LED lights are off

【Prompt Information】-

【Common Mistake】 When the configured Session id does not exist, the following error message will be prompted:

```
AC-FS(config-ap)#quiet-mode session 1
invalid session!
```

【Platform Description】 -

13 LICENSING

13.1license copy

Back up the authorization file.

license { copy-all | copy-file filename } { flash: | usb0: } [target-filename]

【Parameter Description】

Parameter	Description
copy-all	Back up all permanent entitlements on the system.
copy-file	The authorization specified by filename on the backup authorization. filename can be an installed authorization file name or a feature name. When filename is a feature name, all installed authorization files under the feature are backed up.
filename	The name of the authorization file or attribute installed on the system.
flash:	Specifies the location of the authorization file on the internal flash file system.
usb0:	Specifies the location of the authorization file on the USB file system.
target-filename	Specify the authorization file name.

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 4

【Usage Guide】 When backing up all the authorization files in the system, the tar file is generated. This command does not require authorization.

copy-file can back up a single authorization file or all authorization files for a feature.

【Configuration Example】Under the rg-license-lics path (the path must exist) of the backup system to the USB flash drive, the license compressed package is named lics.tar

```
AC-FS#lic copy-all usb0:rg-license-lics/lics.tar
Success to copy all permanent license.
```

【Verification】 You can use dir to determine the generated license file compressed package. After decompression, compare it with the license file name displayed in the installed license Field of each permanent license feature in show license all-license to check whether the

backup is correct.

The installed license Field is only available for multi-instance authorization. The file name of the internal backup of the multi-instance authorization system is determined by the id number of the multi-instance authorization. Single-instance authorization Since there is at most one authorization file in the system at the same time, the internal authorization file backup is directly named after the feature name. In this example, 19881021.lic, 19881023.lic The id number is embedded in the authorization file. Since the package is stored in folders according to the characteristics, the user can still distinguish which characteristic an authorization file corresponds to.

【Prompt Information】 1: When backing up all authorizations, there is no authorization to back up on the system

```
Copy failed, there's no permanent license in the system.
```

2: Successfully back up all authorizations of the system

```
Success to copy all permanent license.
```

3: If there is no specified feature or authorization file on the device, an error will be prompted.

```
Copy failed, there's no such service or license installed in the system.
```

4: If the specified authorization is time-sensitive, it will prompt failure.

```
Copy failed, the license is temporary.
```

5: Successfully back up the specified authorization

```
Success to copy license vsd.lic.
```

【Common Mistake】 1. The specified authorization or specified file does not exist on the system.

2. The authorization specified to be backed up is temporary and cannot be backed up.

【Platform Description】 -

13.2license grace-period

Set the early warning time for authorization invalidation.

license grace-peroid license days

Turn off Warning Before Failure.

no license grace-peroid filename

Restore Default Configuration.

default license grace-peroid filename

【Parameter Description】

Parameter	Description
filename	Authorized property name.
days	Limit point of warning before failure..

【Default Configuration】 Among the two values of 120 days and half of the evaluation authorization time, the default value is the smaller value.

【Command Mode】 Privileged mode

【Default Level】 4

【Usage Guide】 When an authorization timeout period is less than the friendly period warning value, a warning will be generated once a day; on the day before the authorization expires, a warning will be generated every hour. Warnings are sent as logs or SNMP TRAPs.

This command does not require authorization.

The early warning time can be set only after the evaluation authorization, and the permanent authorization does not need to be set.

【Configuration Example]】 1: Set the number of days for the friendly period warning to 100 days.

```
AC-FS#license grace-period LIC-WLAN-AP-8
Success to set alarm starting point of license LIC-WLAN-AP-8.
```

【Verification】 After the authorization period is less than 100 days, a warning Prompt Information will appear at regular intervals.

【Prompt Information】 1: Set successfully.

```
Success to set alarm starting point of license LIC-WLAN-AP-8.
```

2: The specified authorization does not exist in the system.

```
There's no license abc in the system.
```

【Common Mistake】 The specified authorization does not exist in the system.

【Platform Description】 -

13.3 license install

Install a license.

license install { flash: | usb0: } filename

【Parameter Description】

Parameter	Description
flash:	Specifies the location of the authorization file on the internal flash file system.
usb0:	Specifies the location of the authorization file on the USB file system.
filename	Specify the authorization file name.

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 4

【Usage Guide】 The authorization file name can be modified. This command does not require authorization.

【Configuration Example]】Obtain the device host number, register to obtain the authorization file, and install the authorization file:

```
AC-FS#show license hostid
8708EH5F00042
AC-FS#license install usb0: WLAN-AP-8.lic
License file install success, service name: LIC-WLAN-AP-8.
```

【 Verification 】 Use show license all-license to check whether there is a corresponding authorized function name in the displayed information to determine whether it is installed correctly.

【Prompt Information】 1: The authorization file does not exist:

```
Install failed: no such file or directory.
```

2: The authorization file check is illegal:

```
Install failed: the install license may be wrong.
```

3: A newer authorization than the authorization file to be installed already exists in the system:

```
Install failed: the system already has a same license which is newer.
```

4: Repeat the installation of the authorization file:

```
Install failed: the license has been installed before.
```

5: The authorization is a temporary authorization, and the same permanent authorization already exists in the system

```
Install failed: The system already has a same permanent license.
```

6. The authorization file is installed successfully (in this example, the authorization of the feature LIC-WLAN-AP-8 is used):

```
License file install success, service name: LIC-WLAN-AP-8
```

7. The license is installed successfully, and the license is converted into a permanent license (in this example, the license of the feature LIC-WLAN-AP-8 is used as an example)

```
License file install success, service name: LIC-WLAN-AP-8.
The license turns to be permanent.
```

8. The license is installed successfully, and the license is about to expire (less than 30 days) (in this example, the license of the feature LIC-WLAN-AP-8 is used),

```
License file install success, service name: LIC-WLAN-AP-8.;
The installed license is approaching deadline, less than 30 days.
```

【Common Mistake】 1. The specified authorization file does not exist.

2. The authorization document is illegal.

3. The pre-installed license is longer than the system has.

4. Install the same authorization file repeatedly.

5. The temporary license is pre-installed, and the system has a permanent license installed.

【Platform Description】 -

13.4 license uninstall

Uninstall the license.

license uninstall { all | license [filename] }

【Parameter Description】

Parameter	Description
all	Uninstall all authorization files in the system.

license	Authorization name to uninstall.
filename	filename to uninstall.

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 4

【Usage Guide】 This command does not require authorization.

When the license-related features are running, the license will not take effect immediately after the license is uninstalled.

After the license is uninstalled, it cannot be restored. It is recommended to back up the license file before uninstalling..

【Configuration Example】Uninstall authorization on the system.

```
AC-FS#license uninstall LIC-WLAN-AP-8
Uninstall LIC-WLAN-AP-8 success.
```

【Verification】Use the show license all-license command to view the Service name Field. If the uninstalled function name does not appear, the uninstallation is successful.

【Prompt Information】 1: Error message: There is no specified authorization on the device (in this example, the specified authorization name is defd).

```
Uninstall failed: there's no license defd in the system.
```

2: Error message: There is no specified authorization file for the specified feature on the device (in this example, the specified feature is LIC-WLAN-AP-32, and the specified authorization file name is 123.lic).

```
Uninstall failed: there's no license 123.lic of service LIC-WLAN-AP-32 in the system..
```

3: Error message: Uninstall the single authorization file of the single-instance authorization feature.

```
Uninstall failed: single instance license does not support license based uninstalling.
```

4. The license uninstallation is successful (in this example, the feature LIC-WLAN-AP-8 is used):

```
Uninstall LIC-WLAN-AP-8 success.
```

5. A single file in a license is successfully uninstalled (in this example, LIC-WLAN-AP-32 is the license feature name, and AP32_1.lic is a

single license file):

```
Uninstall license AP32_1.lic of service LIC-WLAN-AP-32 success.
```

【Common Mistake】 1. The authorization of the specified authorization feature has not been installed on the device.

2. The specified authorization file does not exist under the specified authorization feature on the device.

3. Pre-uninstall an authorization file under the single-instance feature (single-instance authorization does not support the uninstallation of a single file).

【Platform Description】 -

13.5license unbind

Unbind an authorization.

license unbind pak

【Parameter Description】

Parameter	Description
pak	Specifies the authorization code.

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 4

【Usage Guide】The function of this command is to release the binding relationship between an authorization file and the corresponding device. Before the user can unbind on the webpage, he must first unbind with this command on the desired device.

After successfully unbinding, you will get a string of verification codes. This verification code is required to unbind on the webpage.

【Configuration Example]】Unbind the authorization with the authorization code LIC-FCOE00000012268888

```
AC-FS#license unbind LIC-FCOE00000012268888
Success to unbind license LIC-FCOE00000012268888.
The verification string is 775719468737BA269825589557F558657575B5D5D5D5D785782598859765A8355855.
```

【Verification】You can use the show license command to check whether there is a license corresponding to the specified authorization

code.

```
AC-FS#show license all-license
```

```
Searching license in the system...
1.Service name: LIC-VSD
    Attribute: Permanent, Releasable
Licensed serial number: LIC-VSD00000012268888
```

【Prompt Information】 1: There is no matching authorization in the system:

Unbind failed: not match license found.

【Common Mistake】 There is no matching authorization in the system.

【Platform Description】 -

13.6license update

Update an authorization.

license update { flash: | usb0: } filename

【Parameter Description】

Parameter	Description
flash:	Specifies the location of the authorization file on the internal flash file system.
usb0:	Specifies the location of the authorization file on the USB file system.
filename	Specify the authorization file name.

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 4

【Usage Guide】 This command does not require authorization, and the authorization file name can be modified.

【Configuration Example]】Update the temporary authorization on the system to a permanent authorization

1. Obtain the permanent authorization file WLAN-AP-8_perm.lic of LIC-WLAN-AP-8 by purchasing and other means, put WLAN-AP-8_perm.lic in the usb, and connect the usb to the device;

2. Update the authorization of the feature LIC-WLAN-AP-8.

```
AC-FS#license update usb0: WLAN-AP-8_perm.lic
License file update success, temporary license LIC-WLAN-AP-8 changes into permanent.
```

【**Verification**】You can use the show license command to check whether the Attribute Field authorization attribute is permanent to determine whether the corresponding attribute has been updated.

```
AC-FS(config)#show license all-license
Searching license in the system...
1.Service name: LIC-WLAN-AP-8
    Attribute: Permanent, Releasable
    Licensed serial number: LIC-WLAN-AP-800000012268888
```

【**Prompt Information**】 1: The authorization file does not exist:

```
Update failed: No such file or directory.
```

2: The authorization file check is illegal:

```
Update failed: the update license may be wrong.
```

3: The preinstalled authorization files are older than those present in the system:

```
Update failed: the new installed license is older than the system one
```

4: The license has been installed before:

```
Update failed: the license has been installed before.
```

5: Temporary authorization cannot replace permanent authorization:

```
Update failed: the period license cannot replace permanent license.
```

6: No authorization has been installed before the authorization feature corresponding to the pre-installed authorization, please install it first:

```
Update failed: now the system does not have the license.
               Try "license install" instead.
```

7. The update is successful, and an evaluation authorization is converted into a permanent authorization (in this example, the authorization of the feature LIC-WLAN-AP-8 is used):

```
Update success, temporary license LIC-WLAN-AP-8 changes into permanent.
```

【Common Mistake】 1. The authorization file is not the device's.

2. Pre-replace the newer license with the older license.

3. The updated license has been installed before.

4. Pre-use temporary authorization instead of permanent authorization.

5. When updating the authorization, the corresponding authorization feature does not have any authorization installed.

【Platform Description】 -

13.7show license

Check the authorization status of the device.

show license { all-license | file [license] }

【Parameter Description】

Parameter	Description
all-license	Displays a list of all the installed authorization files in the device.
file filename	Displays an information that specifies the authorization name.

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】 This command does not require authorization and is used to display authorization information in the system

【Configuration Example]】1: Display an authorization information.

```
AC-FS#show license file LIC-WLAN-AP-8
Service  name:  LIC-WLAN-AP-8
Attribute: Temporary, Releasable
Left days: 362
Licensed serial number: LIC-WLAN-AP-800000012268888
```

2. Display all installed license information in the system.

```
AC-FS#show license all-license
Searching license in the system...
Dev 1:
1. Service name: LIC-WLAN-AP-8
    Attribute: Releasable
    [Permanent licenses]     [Licensed serial number]
    19880966.lic             LIC-WLAN-AP-800000012264966
    19880988.lic             LIC-WLAN-AP-800000012264988

    [Temporary license]      [Licensed serial number]
    19880900.lic             LIC-WLAN-AP-800000012264900
    (63 days left)
```

Field Description:

Field	Instruction
Service name	Authorized property name.
Attribute	Some properties of the authorization.
Left days	The remaining days of the authorization period.
Licensed serial number	authorization code.

【Prompt Information】-

【Platform Description】 -

13.8show license hosted

Displays the host number used for authorization.

show license hostid

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】 This command does not require authorization, the serial number is used to uniquely identify a device.

【Configuration Example】1: View the hostid of a device.

```
AC-FS#show license hostid
1234942570021
```

【Prompt Information】-

【Platform Description】 -

13.9show license usage

View the current authorized usage of the system.

show license usage

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】 This command does not require authorization.

【Configuration Example]】1: View detailed information of all PIM interfaces.

```
AC-FS#show  license  usage
Searching license in the system...
 1. Service name: LIC-WLAN-AP-8
```

```
    Attribute: Permanent, Multiple instance, Releasable
    Installed licenses(s): 123.lic
```

Field Description:

Field	Description:
Service name	Authorized property name.
Attribute	Some properties of the authorization.
Left days	The remaining days of the authorization period.

【Prompt Information】-

【Platform Description】 -

13.10show license unbind-code

View the verification code of the unbound authorization of this device

show license unbind-code

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】 This command does not require authorization.

【Configuration Example]】1: View the verification code information that the device has been unbound and authorized.

```
AC-FS#show license unbind-code
LICENSE                                                                    UNBINDING-CODE LIC-
VSD00000012264933     77571FF68737BFF69FF55FF557F55FF57575B595E58587857FF59FF59765AFF55FF5     LIC-
FC0E00000012264966  77571FF68737BFF69FF55FF557F55FF57575B595E5B5B7857FF59FF59765AFF55FF5
LIC-TRILL00000012264988   77571FF68737BFF69FF55FF557F55FF57575B595E5D5D7857FF59FF59765AFF55FF5
```

Field Description:

Field	Description
LICENSE	Unbound authorization code.
UNBINDING-CODE	Unbound verification code.

【Prompt Information】-

【Platform Description】 -

14 USB

14.1show usb

View inserted USB device information.

show usb

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】 If there is a USB device, the device information will be displayed, otherwise there will be no output. If the U disk is directly inserted into the USB port of the device, the ID format displayed by show usb is X, where X is a number, indicating the USB port number; The ID format is X-Y, where X and Y are numbers, X represents the USB port number of the device, and Y represents the slot number of the HUB.

【Configuration Example]】1: Insert the U disk directly into the USB port of the device, the following is the information displayed on the USB:

```
AC-FS# show usb
Device: Mass Storage
ID: 0
URL prefix: usb0
Disk Partitions:
usb0(type:FAT32)
Size : 131,072,000B(125MB)
Available size:  1,260,020B(1.2MB)

Device: Mass Storage
ID: 1
URL prefix: usb1
Disk Partitions:
usb1(type:FAT32)
Size : 131,072,000B(125MB)
Available size:  1,260,020B(1.2MB)
```

Field Description:

Field	Description

ID	Device No.
URL prefix	Indicates the access prefix of the U disk.
Size	Indicates the accessible space on the USB drive.
Available size	Indicates the remaining space on the USB flash drive.

2: The U disk is inserted into the HUB port, the HUB is inserted into the USB port of the device, and the following is the information displayed on the USB:

```
AC-FS# show usb
Device: Mass Storage
ID: 0-3
URL prefix: usb0-3
Disk Partitions:
usb0-3(type:vfat)
Size:15789711360B(15789.7MB)
Available size:15789694976B(15789.6MB)

Device: Mass Storage
ID: 0-4
URL prefix: usb0-4
Disk Partitions:
usb0-4(type:vfat)
Size:15922782208B(15922.7MB)
Available size:14861926400B(14861.9MB)
```

Field Description:

Field	Description
ID	Device No. 0 means the 0th USB port of the device, 3, 4 means the slot number of the HUB.
URL prefix	Indicates the access prefix of the U disk.
Size	Indicates the accessible space on the USB drive.
Available size	Indicates the remaining space on the USB flash drive.

【Prompt Information】-

【Platform Description】 -

14.2usb remove

Remove the USB device.

usb remove device-id

【Parameter Description】

Parameter	Description
device-id	Device number, which is the ID number in the USB display information. The device number can be obtained via the show usb.

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】 Before unplugging the USB device, you need to use the command to remove the device, in case the system is using the device and cause an error. If the device is removed successfully, the system will print out a prompt before unplugging the device. If the removal fails, and the USB device is in use by the system at the moment, you must wait for a while before performing the removal operation.

【Configuration Example]】1: The following is to remove the USB device shown in the above example:

```
AC-FS# usb remove 0
OK, now you can pull out the device 0.
```

At this point, the USB device can be unplugged.

【Verification】After the command is executed successfully, show usb will not be able to see the relevant information of the usb device. If the command execution fails, show usb can also see the relevant information of the usb device.

【Prompt Information】 1. After executing the uninstall command, if the execution is successful, the system will print out the following information:

OK, now you can pull out the device 0

2. After executing the uninstall command, if the execution fails, the system will print the following information:

Device is busy now, try again few minutes later.

【Common Mistake】 Print Device is busy now, try again few minutes later. Description the device is being used, please close all operations using the device first. For example, after the previous cd usb0:/ operation, it did not exit, and it will prompt failure when

executing usb remove 0. At this time, please execute the cd flash:/ operation, switch the current path to flash, and then execute usb remove 0.

【Platform Description】 -

15 PKG_MGMT

15.1patch active

Activate the patch for the patch to take effect.

patch active

【Parameter Description】-

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】The activation operation can only be performed after the patch is installed successfully. After the patch is activated, the patch is actually used by the system. This command is used to temporarily activate the hot patch, and the patch will become invalid after the device restarts.

【Configuration Example】1. Box device activation patch.

```
AC-FS#patch active
 Active the patch package success
```

2. Rack device activation.

```
AC-FS#patch active slot 8
 [Slot 8]:
 Active the patch package success
```

【Verification】Use show patch to view patch information.

【Prompt Information】 1. Successful execution prompt:

Active the patch package success

2. If the execution fails, an error is displayed. The patch package is not installed. The hot patch package needs to be installed first:

Patch not installed

3. The patch package has been activated, no need to execute this command:

The patch status is already active or running

4. If there is any problem with the patch package itself, please contact customer service:

Cannot find the package's scripts file

【Common Mistake】 1. The current device has not yet installed hot patches.

2. The hot patch for the current device is already active.

【Platform Description】 -

15.2patch deactive

Invalidate the patch effect.

patch deactive

【Parameter Description】-

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】 Only active patches can perform this operation, and this operation will invalidate the effect of the patch.

【Configuration Example】1. Boxed devices invalidate the patch.

```
AC-FS#patch deactive
 Deactive the patch package success
```

2. Rack equipment invalidates the patch.

```
AC-FS#patch deactive slot 8
 [Slot 8]:
Deactive the patch package success
```

【Verification】Use show patch to view patch information.

【Prompt Information】 1. Successful execution prompt:.

Deactive the patch package success;

2. If the execution fails, an error is displayed. The patch package is not installed. The hot patch package needs to be installed first:

Patch not installed

3. The function of the patch package has expired, so there is no need to execute this command:

The patch is not in active or running status

4. If there is any problem with the patch package itself, please contact customer service:

Cannot find the package's scripts file

【Common Mistake】 1. The current device has not yet installed hot patches.

2. The hot patch for the current device has expired.

【Platform Description】 -

15.3 patch delete

Remove the patch.

patch delete

【Parameter Description】-

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】 This command is used to clear the existing hotfix package on the device

【Configuration Example】1. The boxed device clears the installed hotfix package.

```
AC-FS# patch delete
 Clear the patch patch_bridge success
 Clear the patch success
```

2. The rack device clears the installed hotfix package.

```
AC-FS# patch delete slot M1
[Slot M1]:
Clear the patch patch_bridge success
Clear the patch success
```

【Verification】Use show patch to view patch information.

【Prompt Information】 1. Successful execution prompt:

Clear the patch success

2. The patch package is not installed, you need to install the hot patch package first:

Patch not installed

【Common Mistake】 ↑ The current device has not yet installed hot patches

【Platform Description】 -

15.4patch running

Make the patch effect permanent.

patch running

【Parameter Description】-

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】The activation operation can only be performed after the patch is installed successfully. After the patch is activated, the patch is actually used by the system. This command is used to permanently activate the hot patch.

【Configuration Example】1. Box device activation patch.

```
AC-FS#patch running
The patch on the system now is in running status
```

2. Rack device activation.

```
AC-FS#patch running slot M1
[Slot M1]:
The patch on the system now is in running status
```

【Verification】 Use show patch to view patch information.

【Prompt Information】 1. Successful execution prompt:

The patch on the system now is in running status

2. If the execution fails, an error is displayed. The patch package is not installed. The hot patch package needs to be installed first:

Patch not installed

3. The function of the patch package has expired, so there is no need to execute this command:

The patch is not in active or running status

4. If there is any problem with the patch package itself, please contact customer service:

Cannot find the package's scripts file

【Common Mistake】 1. The current device has not yet installed hot patches

2. The hot patch for the current device is already active

【Platform Description】 -

15.5 show component

Displays all components installed on the current device and information about each component.

show component [component _name]

【Parameter Description】

Parameter	Description

component _name	Component name. When this Parameter value does not exist, it displays basic information for all installed components in the device. When this Parameter value is present, it is used to display the details of the corresponding component, verify whether the component content is complete, and detect whether the component works properly.

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】 This command includes two forms, with component_name Parameter and without this Parameter. Before upgrading or uninstalling components, users often need to know all the installed components and component version information of the current device. In this case, the show component command without Parameter should be used. When the user needs to learn more about a component, use the show component command with Parameter to get the detailed information of the corresponding component. Through this information, the user can easily understand the working status of the component, and judge whether the content of the component has been damaged by man, which is of great significance in eliminating functional failures and ensuring the safe and reliable operation of the component.

Some components will modify their default configuration files during use. Although this is a normal situation and does not belong to malicious damage, the show component command can only determine that the component files have changed during use, and cannot distinguish whether it is malicious damage. Further self-judgment is required.

【Configuration Example】 1. The box device displays all components currently installed and information about each component.

```
AC-FS# show component
Package  :sysmonit
    Version:1.0.1.23cd34aa      Build time: Wed Dec  7 00:58:56 2013
    Size:12877    Install time :Wed  Mar 5 14:23:12 2012
    Description: this is a system monit package
    Required packages: None
----------------------------------------------------------------------------------------------------
Package:bridge
    Version:2.0.1.37cd5cda      Build time: Wed Dec  7 00:54:56 2013
    Size:23245    Install time :Wed  Mar 5 14:30:12 2012
    Description: this is a bridge package
    Required packages: None
----------------------------------------------------------------------------------------------------
```

Using this command form, you can obtain all the components installed in the device and the basic information of the components, which provides the basis for the user to decide whether to upgrade or uninstall the components.

Field Description:

Field	Description
Package	component name.
Version	Component version number.
Build time	The time when the component was compiled on the server.
Size	The size of the component's contained content.
Install time	When the component was installed on the device.
Description	Simple Description of Component Function.
Required packages	Which components do you depend on.

2. The rack-mounted device displays the information of the currently installed functional components.

```
AC-FS#show component slot 8 AC-FS#*
[Slot 8]:
Package : utils-system
     Version: 1.0.0.433ef8d         Build time: Sun May 19 19:22:54 2013
     Size: 823936   Install time: Sun May 19 19:27:04 2013
     Description: utils system compile
     Required packages: None


----------------------------------------------------------------------------

Package : tcl-expect
     Version: 1.0.0.433ef8d         Build time: Sun May 19 19:19:18 2013
     Size: 3474153          Install time: Sun May 19 19:27:04 2013
     Description: tcl & expect packages
     Required packages: None
----------------------------------------------------------------------------
```

3. The box device displays information about the specific components installed in the current device.

```
AC-FS# show component bridge
package:bridge
     Version: 2.3.1.1252ea       Build time: Wed Dec  7 00:54:56 2013
```

```
    Size:26945    Install time : Wed Mar 19:23:15 2012
    Description:this is a bridge package
    Required packages: None
    Package files:
       /lib64
       /lib64/libbridge.so
       /sbin
       /sbin/bridge

   Package file validate: [OK]
   Required relationship verify: [OK]
```

In addition to the basic information of the components, it also includes:

Field Description:

Field	Description
Package file validate	Check the integrity of the file.Show results [OK] if all component files are normal; if some of the files are lost or modified, show results [ERR] and specify which The file is lost or is modified.
Required package	List all dependent components for the component, mark "[OK]" if the dependent component is installed, "[ERR]" if the dependent component is not installed and detail Instruction which dependent component has not installed and dependent version information of the component.
Package files	Lists all of the files contained in the package.

【Prompt Information】 After successful execution, the information of each component in the device is displayed:

```
Package  :sysmonit
     Version:1.0.1.23cd34aa      Build time: Wed Dec  7 00:58:56 2013
     Size:12877    Install time :Wed  Mar 5 14:23:12 2012
     Description: this is a system monit package
     Required packages: None
-------------------------------------------------------------------------------------------------------
Package:bridge
     Version:2.0.1.37cd5cda      Build time: Wed Dec  7 00:54:56 2013
     Size:23245    Install time :Wed  Mar 5 14:30:12 2012
     Description: this is a bridge package
     Required packages: None
-------------------------------------------------------------------------------------------------------
```

【Platform Description】 -

15.6 show patch

Displays information about hotfix packages installed on the device.

show patch [patch _name]

【Parameter Description】

Parameter	Description
patch_name	Patch name. When this Parameter value does not exist: The command displays basic information for all installed patches in the device. When this Parameter value exists: the command is used to display the patch, the component content is complete, etc.

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】 This command can view the installed patches and patch information

【Configuration Example】1. The boxed device shows that all patches are currently installed.

```
AC-FS# show patch
patch package patch_install installed in the system, version:pa1
Package : patch_bridge
status: running
Version: pa1       Build time: Mon May 13 09:03:07 2013
     Size: 277      Install time: Tue May 21 03:07:17 2013
     Description: a patch for bridge
     Required packages: None
```

Using this command form, you can obtain the basic information of all patches installed in the device.

Field Description:

Field	Description
Package	Patch name.
status	Patch status.
Version	Component patch version information.

Build time	When the patch was compiled on the server.
Size	The patch contains the size of the content.
Install time	The time when the device installed the patch.
Description	Patch feature of the simple description.

2. The rack-mounted device displays information about the currently installed patches.

```
AC-FS#show patch slot 8
[Slot 8]:
```

```
Patch package patch_install installed in the system, version:pa1
Package : patch_test
Status: running
     Version: 1.0.0.05151504
     Build time: Wed May 15 07:04:28 2013
     Size: 1804
     Install time: Thu Jan  1 00:56:43 1970
     Description: Experimentation
     Required packages: None
```

3. The box device displays the specific patch information installed on the current device.

```
AC-FS# show component bridge
package:bridge
     Version: 2.3.1.1252ea       Build time: Wed Dec  7 00:54:56 2011
     Size:26945    Install time : Wed Mar 19:23:15 2012
     Description:this is a bridge package
     Required packages: None
     Package files:
        /lib64
        /lib64/libbridge.so
        /sbin
        /sbin/bridge

    Package file validate: [OK]
```

In addition to the basic patch information, it also includes:

Field Description:

Field	Description

Package file validate	Verify the integrity of the patch include files. If all files are normal, display the result [OK]; if some files are missing or modified, display the result [ERR], and clearly indicate which file is missing or modified.
Package files	List all files included in the patch package

【Prompt Information】 Displays the patch information that exists in the device after execution.

```
Patch package patch_install installed in the system, version:pa1
Package : patch_bridge
 Status: running
 Version: pa1       Build time: Mon May 13 09:03:07 2013
     Size: 277      Install time: Tue May 21 03:07:17 2013
     Description: a patch for bridge
     Required packages: None
```

【Platform Description】 -

15.7 show upgrade file

Displays information about the installation package files stored in the device file system.

show upgrade file url

【Parameter Description】

Parameter	Description
url	Install the local url path where the package file is stored.

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】 After downloading the installation package file to the local file system, you can use this command to view the main information of the installation package in advance.

Rack packs are not supported by this command.

【Configuration Example】1. Display installation package file information.

```
AC-FS# show upgrade file flash://bridge_eg1000m_2.3.1.1252ea-1.mips.rpm
Name : bridge
Version:1.0.1.23cd34aa
Package type      : common component
Support target  : eg1000m
Size              : 26945
Build time        : Wed Dec 7 00:54:56 2013
Install date      : (not installed)
Description  : this is a bridge package
Package files :
    Package files:
       /lib64
       /lib64/libbridge.so
       /sbin
       /sbin/bridge
```

Use this command to get the in-package information.

Field Description:

Field	Instruction
Name	Package name.
Version	Package release version information.
Package type	Package type.
Support target	Package-supported product Instruction.
Size	The size of the content that is included.
Build time	Package compilation time.
Install date	Package installation date.
Description	Package description information.
Package files	All of the contents contained in the package.

【Prompt Information】 Execute to display the installation package information.

```
Name : bridge
Version:1.0.1.23cd34aa
Package type      : common component
Support target  : eg1000m
Size              : 26945
Build time        : Wed Dec 7 00:54:56 2013
Install date      : (not installed)
Description  : this is a bridge package
Package files :
    Package files:
       /lib64
       /lib64/libbridge.so
       /sbin
       /sbin/bridge
```

【Platform Description】 -

15.8 show upgrade history

Display upgrade history information.

show upgrade history

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】-

【Configuration Example】-

【Prompt Information】

```
AC-FS#show upgrade history
Last Upgrade Information:
    Time:         2014-08-31 12:15:03
    Method:       LOCAL
Package    Name:    N18000_RGOS11.0(1)B1_CM_01200616_install.bin
Package Type: Distribution
```

【Platform Description】 -

15.9 show upgrade peer

Displays the upgrade status of the staging device.

show upgrade peer {all | ip-address} status

【Parameter Description】

Parameter	Description
all	All graded equipment.
ip-address	Specifies the IP address of the graded device.

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】-

【Configuration Example】1: Display the upgrade status of the classification device.

```
AC-FS#show upgrade peer all status
peer self
        Device type        : ws5708
        Status             : ready
peer 10.1.1.20
        Device type        : ws5708
        Status             : success
peer 10.1.1.30
        Device type        : ws5708
        Status             : transmission
        Upgrade processing : 20%
```

AC-FS#

【Prompt Information】 Execute the prompt for each hierarchical equipment upgrade status.

```
peer self
      Device type       : ws5708
      Status             : ready peer
10.1.1.20
      Device type       : ws5708
      Status             : success peer
10.1.1.30
      Device type       : ws5708
      Status             : transmission
          Upgrade processing : 20% AC-
FS#
```

【Platform Description】 This command is only supported by graded devices.

15.10upgrade

Install and upgrade the installation package in the local file system.

upgradeurl [force]

【Parameter Description】

Parameter	Description
url	The url is the local path for the installation package storage. This command is used to upgrade the installation packages stored within the device.
force	The force indicates a mandatory upgrade

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】 This command supports each subsystem component installation package, rack equipment installation package, functional component installation package, and hot patch package. Before using this command, use the copy command to copy the function package into the device file system.

When this command is used without specifying the range Parameter, the upgrade function will upgrade the matched system components

according to the automatic synchronization configuration.

【Configuration Example】1. Device upgrade main package.

```
AC-FS#upgrade usb0:/eg1000m_main_1.0.0.0f328e91.bin
 Upgrade processing is 10%
 Upgrade processing is 60%
 Upgrade processing is 90%
 Upgrade info [OK]
     Kernel version[2.6.32.91f9d21->2.6.32.9f8b56f]
     Rootfs version[1.0.0.2ad02537->1.0.0.1bcc12e8]
 Upgrade processing is 100%
 Reload system to take effect!
```

2. Equipment upgrade rack package.

```
AC-FS# upgrade usb0:/ca-octeon_11.0(1B2)_20131106_main_install.bin
[Slot M1]:Upgrade processing is 10%

 [Slot 1]:Upgrade processing is 10%

 [Slot M1]:Upgrade processing is 60%

 [Slot 1]:Upgrade processing is 60%

 [Slot M1]:Upgrade processing is 90%

 [Slot M1]:
 Upgrade info [OK]
   Kernel version[2.6.32.abb2b41f170c81->2.6.32.abb2b415749f40]
   Rootfs version[1.0.0.d5f0de03->1.0.0.660e0085]

 [Slot M1]:Restart to take effect !

 [Slot M1]:Upgrade processing is 100%
 [Slot 1]:Upgrade processing is 90%

 [Slot 1]:
 Upgrade info [OK]
   Kernel version[2.6.32.9f8b56f1d45ab2 ->2.6.32.0f48cb9f170c81]
   Rootfs version[1.0.0.2ad02537->1.0.0.1bcc12e8]

 [Slot 1]:Restart to take effect !
```

```
[Slot 1]:Upgrade processing is 100%
[slot: M1]
  device_name: ca-octeon-cm
  status:      SUCCESS
[slot: 1]
  device_name: ca-octeon-lc
  Status:      SUCCESS
```

【Verification】 3. Use show version detail to check whether the subsystem components are upgraded successfully.

4. Use show component to check whether the functional components are upgraded successfully.

5. Use show patch to check whether the hot patch is installed successfully.

【Prompt Information】 1. Tips for successful upgrade:

```
Upgrade info [OK]
```

2. The installation package is invalid or damaged Re-obtain the installation package and execute the upgrade command:

```
Invalid package file
```

3. The device does not support the installation package, re-obtain the installation package and execute the upgrade command

```
Device don't support
```

4. The equipment does not need to be upgraded:

```
The version in device is newer or the same
```

5. If the upgrade space is insufficient, check whether the U disk attached to the device is in good condition:

```
No enough space for decompress
```

6. If there is a serious problem, the system is damaged, please contact customer service:

```
No enough space,rootfs been destroyed. Please upgrade in uboot
```

7. The patch package already exists in the system, and the old patch package needs to be uninstalled first

```
Already exist patch, please uninstall before upgrade
```

8. The patch package is not suitable for this system, replace the patch package:

```
Patch compatibility err
```

9. The device cannot be upgraded with this patch package, and re-obtain the patch package:

```
Patch compatibility err
```

【Common Mistake】-

【Platform Description】 -

15.11 upgrade download tftp

Download and install, upgrade the installation package on the tftp server.

upgrade download tftp:/path

【Parameter Description】

Parameter	Description
path	The path is the path to install the package on the tftp server and the command automatically downloads the installation package from the server and is automatically upgraded.

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】 This command supports each subsystem component installation package, rack equipment installation package, functional component installation package, and hot patch package. Use this command to automatically complete the installation file copy operation and upgrade.

【Configuration Example】1. Upgrade the main package.

```
AC-FS# upgrade download tftp://192.168.201.98/eg1000m_main_1.0.0.0f328e91.bin
Accessing tftp://192.168.201.98/eg1000m_main_1.0.0.0f328e91.bin...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!
Transmission finished, file length 21525888 bytes.
 Upgrade processing is 10%
 Upgrade processing is 60%
 Upgrade processing is 90%
 Upgrade info [OK]
        Kernel version[2.6.32.91f9d21->2.6.32.9f8b56f]
        Rootfs version[1.0.0.2ad02537->1.0.0.1bcc12e8]
 Upgrade processing is 100%
 Reload to take effect!
```

【Verification】6. Use show version detail to check whether the subsystem components are upgraded successfully.

7. Use show component to check whether the functional components are upgraded successfully.

8. Use show patch to check whether the hot patch is installed successfully.

【Prompt Information】 1. Tips for successful upgrade:

```
Upgrade info [OK];
```

2. The installation package is invalid or damaged Re-obtain the installation package and execute the upgrade command:

```
Invalid package file
```

3. The device does not support the installation package, re-obtain the installation package and execute the upgrade command:

```
Device don't support
```

4. The equipment does not need to be upgraded:

```
The version in device is newer or the same
```

5. If the upgrade space is insufficient, check whether the U disk attached to the device is in good condition:

```
No enough space for decompress
```

6. If there is a serious problem, the system is damaged, please contact customer service:

```
No enough space, rootfs been destroyed. Please upgrade in uboot
```

7. The patch package already exists in the system, you need to uninstall the old patch package first:

```
Already exist patch, please uninstall before upgrade
```

8. The patch package is not suitable for this system, replace the patch package:

```
Patch compatibility err
```

9. The device cannot be upgraded with this patch package, and re-obtain the patch package:

```
Some origin component has change
```

【Common Mistake】-

【Platform Description】 -

15.12 upgrade rollback

Roll back the subsystem to the pre-upgrade version.

upgrade rollback

【Parameter Description】-

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】 If the device cannot work normally after upgrading the subsystem, you can use this command. This command can only take effect when the subsystem components were successfully upgraded last time.

The command takes effect after the device restarts, and recursive rollback cannot be implemented by continuously executing this command.

【Configuration Example】 1. A cartridge device rolls back the subsystem to the pre-upgrade version.

```
AC-FS#upgrade rollback
 kernel rollback version[2.6.32.9f8b56f->2.6.32.91f9d21][OK]
 rootfs rollback version[1.0.0.1bcc12e8->1.0.0.2ad02537][OK]
 Rollback success!
 Reload system to take effect!
```

2. A rack device rolls back a subsystem to a pre-upgrade version.

```
AC-FS#upgrade rollback slot M1
 [Slot M1]:
 kernel rollback version[2.6.32.9f8b56f->2.6.32.91f9d21][OK]
 rootfs rollback version[1.0.0.1bcc12e8->1.0.0.2ad02537][OK]
 Rollback success!
 Reload system to take effect!
```

【Verification】 After restarting the device, use show version detail to check whether the subsystem components are successfully rolled back.

【Prompt Information】 1. Success tips:

```
 Rollback success!
 Restart to take effect !
```

2. The subsystem components were not upgraded last time, so the subsystem components cannot be rolled back:

```
Not subsys package last upgrade
```

3. The last upgrade was not successful, so no rollback:

```
Last upgrade err or skip
```

4. The upgrade command has not been executed, or the rollback operation has been executed:

```
Monitor file lost
```

【Common Mistake】 1. The last time was not for the subsystem component upgrade, but the functional component package, hot patch package, etc.

2. A subsystem rollback operation has been performed.

【Platform Description】 -

15.13 clear storage

Clear local installation packages.

clear storage [url]

【Parameter Description】

Parameter	Description
url	The local url directory or full path name that the installation package stores.

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 2

【Usage Guide】 This command can specify to clear a certain installation package or all installation packages in a certain directory. By default, all local installation packages are cleared.

【Configuration Example】

```
AC-FS#clear storage
Remove the whole storage directory?[y/n]y AC-
FS#clear storage usb0
Remove the file or directory usb0 from the storage?[y/n]y
AC-FS#
```

【Verification】View the specified url.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

16 SYS

16.1calendar set

Set the system hardware time.

calendar set [month [day [year]]]

【Parameter Description】

Parameter	Description
hour [:minute [:second]]	Set the system hardware time, hour:minute:second, only the specified hour, minute, and second will be reset, and the omitted part will use the current system setting value.
month	Set the month, the value range is 1~12.
day	Set the date, the value range is 1~31. If this day does not exist in the current month, the date will be calculated backward.
year	Set the year, the value range is 1970~2099.

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】-

【Usage Guide】 9. The time parameter must be entered, and then follow the order of month month, date day, year year parameter, and the latter parameter can be omitted as needed. The omitted Parameter is the current setting value of the system. For example, if the current hardware time is "2012-02-29 09:33:44", only the month and hour are changed, and the others remain unchanged. You can enter the command calendar set 12 5, and the current time becomes "2012-05-29" 12:33:44".

10. If the input day Parameter is within 1~31, but this day does not exist in the month, the date will be calculated backward. For example, there are 29 days in February 2012. If the date is set to February 31, calendar set 11:30 2 31 2012, the system will add two days later by default, and the current hardware time is "2012-03-02 11:30:23".

The set system hardware time acts as UTC time, while the system software time refers to the device local time.

Only devices under vsd0 have this command, and multiple vsds are not supported.

【Configuration Example]】1: Change the current system hardware time (assuming 2012-02-01 18:23:06) to 6 hours, and keep other parameters unchanged.

```
AC-FS# calendar set 6
06:41:39 UTC Fri, Jul 6, 2012
```

2: Change the current system hardware time (assuming 2012-02-01 18:23:06) to 6 hours and 42 minutes, and keep other parameters unchanged.

```
AC-FS# calendar set 6:42
06:42:27 UTC Fri, Jul 6, 2012
```

3: Change the current system hardware time (assuming 2012-02-01 18:23:06), change the month and date to March 2, and leave other parameters unchanged.

```
AC-FS# calendar set 18 3 2
18:43:05 UTC Fri, Mar 2, 2012
```

Since the hour Parameter in the command is a mandatory Field, if the parameter does not need to be changed, enter the clock value consistent with the current hour: enter the clock value 18, and then enter the month and date "3 2"

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

16.2clock read-calendar

Set the system to synchronize the software time according to the hardware time.

clock read-calendar

【Parameter Description】-

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】-

【Usage Guide】This command is only available for devices under vsd0, and multiple vsds are not supported.

With this command, the system will generate the corresponding software time from the current hardware system time according to the device time zone and daylight saving time settings.

【Configuration Example】1: Configure the system to synchronize the software time according to the hardware time.

```
AC-FS# clock read-calendar
Set the system clock from the hardware time.
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

16.3clock set

Set the system software time.

clock set [month [day [year]]]

【Parameter Description】

Parameter	Description
hour [:minute [:second]]	Set the system software time, hour: minute: second, only the specified hour, minute, and second will be reset, and the omitted part will use the current setting value of the system.
month	Set the month, the value range is 1~12.
day	Set the date, ranging from 1 to 31. If this day does not exist in the current month, the date will be calculated backwards.
year	Set the year, the value range is 1970~2099.

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】-

【Usage Guide】 Ð The time parameter must be entered, and then follow the order of month month, date day, year year parameter, and the latter parameter can be omitted as needed. The omitted Parameter is the current setting value of the system.

For example, if the current system software time is "2012-02-29 09:33:44", only the month and hour are changed, and the others remain unchanged. You can enter the command clock set 12 5, and the current time becomes "2012-05- 29 12:33:44"

11. If the input day Parameter is within 1~31, but this day does not exist in the month, the date will be calculated backward.

For example, there are 29 days in February, 2012. If the date is set to February 31, clock set 11:30 2 31 2012, the system will add two days later by default, and the current system software time is "2012-03- 02 11:30:23".

Only devices under vsd0 have this command, and multiple vsds are not supported.

【Configuration Example】】1: Change the current system software time (assuming 2012-02-01 18:23:06) to 6 hours, and keep other parameters unchanged.

```
AC-FS# clock set 6
06:48:13 CST Fri, Mar 2, 2012
```

2: Change the current system software time (assuming 2012-02-01 18:23:06) to 6 hours and 42 minutes, and keep other parameters unchanged.

```
AC-FS# clock set 6:42
06:42:31 CST Fri, Mar 2, 2012
```

3: Change the current system software time (assuming 2012-02-01 18:23:06), change the month and date to March 2, and keep other parameters unchanged.

```
AC-FS# clock set 18 3 2
18:42:48 CST Fri, Mar 2, 2012
```

Since the hour Parameter in the command is a required Field, if the Parameter does not need to be changed, enter the clock value consistent with the current hour: enter the clock value 18, and then enter the month and date "3 2".

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

16.4clock summer-time

Set daylight saving time.

clock summer-time zone start start-month [week|last] start-date hh:mm end end-month [week| last]

end-date hh:mm [ahead hours-offset [minutes-offset]

Turn off daylight saving time.

no clock summer-time

【Parameter Description】

Parameter	Description
zone	The name of the daylight saving time can only be [A~Z][a~z], with no restrictions on upper and lower case. The name length is 3~31.
start	Keyword for the start time when daylight saving time is in effect.
start-month	Start month, the value range: January, February, March, April, May, June, July, August, September, October, November, December. There is no restriction on upper and lower case, and it is not necessary to enter complete words, such as: Febr, FebRu, etc.
week	The starting week number of the starting month. The value range is 1~5.
last	Specified as the last week of a month.
start-date	The day of the week of the starting week of the starting month, the value range is: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday. There is no upper or lower case limit, and complete words are not required. For example: Wed, WeDne, etc.
hh:mm	time, hours, minutes.
end	The end time keyword for which daylight saving time is in effect.
end-month	End month, the value range: January, February, March, April, May, June, July, August, September, October, November, December. There is no restriction on upper and lower case, and it is not necessary to enter complete words, such as: Febr, FebRu, etc.
ahead	The keyword of how much time the daylight saving time is faster than standard time when daylight saving time is in effect. . If not set, the default is 1 hour faster.
hours-offset	The number of hours ahead of standard time. The value range is 0~12. Setting the time ahead of daylight saving time to 00:00 is not allowed.
minutes-offset	The number of minutes ahead of standard time. The value range is 0~59. If hours-offset is already set to 0, minutes-offset is not allowed to also be set to 0

【Default Configuration】-

【Command Mode】 Configuration mode

【Default Level】-

【Usage Guide】

Only devices under vsd0 have this command, and multiple vsds are not supported.

【Configuration Example]】1: If you live in a place, the time zone name is ABC, and the standard time is 8:15 ahead of UTC time, which is GMT+08:15. The daylight saving time period is from the first Saturday in February to the third Monday in May, and the daylight saving time period is 01:20 ahead of standard time. The daylight saving time period is 09:35 ahead of UTC, but the non-daylight saving time period is still 08:15 ahead of UTC.

```
AC-FS(config)# clock timezone ABC 8 15 Set time
zone name: ABC (GMT+08:15) AC-FS(config)#show
clock
16:39:16 ABC Wed, Feb 29, 2012 AC-
FS(config)#show calendar 08:24:35
GMT Wed, Feb 29, 2012

AC-FS(config)# clock summer-time TZA start Feb 1 sat 2:00 end May 3 Monday 18:30 ahead 1 20
*May 10 03:45:58: %SYS-5-CLOCKUPDATE: Set summer-time: TZA from February the 1st Saturday at 2:00 TO May the 3rd
Monday at 18:30, ahead 1 hour 20 minute
Set summer-time: TZA from February the 1st Saturday at 2:00 TO May the 3rd Monday at 18:30, ahead1 hour 20 minute

AC-FS# show clock
18:00:08 TZA Wed, Feb 29, 2012

# If the time is set to off-daylight saving time, the time zone name is
converted back to ABC AC
-FS#clo set 18 1 1
*Jan 1 18:00:09: %SYS-5-CLOCKUPDATE: Set system clock: 18:00:09 ABC Sun, Jan  1, 2012 Set system clock:
18:00:09 ABC Sun, Jan  1, 2012
AC-FS#show clock
18:00:12 ABC Sun, Jan  1, 2012
```

2: The default daylight saving time period is 1 hour faster than the standard time, and the parameters after ahead and ahead can be omitted. For example, set daylight saving time from 2:00 AM on the first Sunday in April to 2:00 AM on the last Sunday in October, 1 hour ahead of standard time.

```
AC-FS(config)#clo summer-time PDT start April 1 sunday 2:00 end October last Sunday 2:00
*May 10 03:15:05: %SYS-5-CLOCKUPDATE: Set summer-time: PDT from April the 1st Sunday at 2:00 TO October
```

3: Turn off daylight saving time.

```
AC-FS(config)#no clock summer-time
*Jan 1 18:01:09: %SYS-5-CLOCKUPDATE: Set no summer time.
Set no summer time.
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

16.5clock timezone

Set the time zone.

clock timezone [name hours-offset [minutes-offset]]

Turn off time zone settings.

no clock timezone

【Parameter Description】

Parameter	Description
name	Time zone name, only [A~Z] [a~z], unlimited case. The name length is 3 to 31.
hours-offset	Hour value of the time difference. Indicates UTC time with fast or slow hours-offset with a value range of [-12,12], negative numbers indicate slower than hardware time and positive numbers faster than hardware time If slower than UTC time, add "-" before hours-offset Parameter.
minutes-offset	Minutes value of the time difference. The values range from 0 to 59.

【Default Configuration】 -

【Command Mode】 Configuration mode

【Default Level】-

【Usage Guide】This command is only available for devices under vsd0, and multiple vsds are not supported.

【Configuration Example]】1: Set the time zone name to CST, and the software time is 8 hours faster than the hardware time.

```
AC-FS(config)# clock timezone CST 8
Set time zone name: CST (GMT+08:00)

AC-FS# show clock
18:00:17 CST Wed, Dec 5, 2012
```

2: Set the time zone name TZA, the software time is 06:13 slower than the hardware time.

```
AC-FS(config)# clock timezone TZA -6 13
Set time zone name: TZA (GMT-06:13)
```

3: Turn off the time zone setting.

```
AC-FS(config)# no clock timezone
Set no clock timezone.
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

16.6clock update-calendar

Set the system to synchronize the hardware time according to the software time.

clock update-calendar

【Parameter Description】-

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】-

【Usage Guide】This command is only available for devices under vsd0, and multiple vsds are not supported.

With this command, the system will generate the corresponding hardware time from the current software system time according to the device time zone and daylight saving time settings.

【Configuration Example】1: Set the system to synchronize the hardware time according to the software time.

```
AC-FS# clock update-calendar
Set the hardware time from the system clock.
```

2: Set the hardware time, the time zone is set to GMT+5:10, and there is no daylight saving time setting, that is, the hardware time is 5:10 slower than the software time.

```
AC-FS# show clock
09:30:21 TSZ Wed, Feb 29, 2012

AC-FS# clock update-calendar
Set the hardware time from the system clock.

AC-FS#show    calendar
04:20:25 UTC Wed, Feb 29, 2012
```

3: Set the hardware time. If the time is set to GMT+5:10, the daylight saving time is set from the first Monday of February 1 to the second Sunday of June 1, which is 1 hour and 15 minutes ahead, that is, in daylight saving time During this time, the hardware time is 6:25 slower than the software time.

```
AC-FS# show clock
09:30:02 TSZ Wed, Feb 29, 2012

AC-FS# clock update-calendar
Set the hardware time from the system clock.

AC-FS#show    calendar
03:05:08 UTC Wed, Feb 29, 2012
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

16.7cpu high-watermark set

Displays and sets the maximum watermark that controls the total CPU usage on the core, and enables monitoring.

cpu high-watermark set [[up up-value] [down down-value]]

Turn off CPU usage monitoring.

no cpu high-watermark set

Restore Default Configuration.

default cpu high-watermark set

【Parameter Description】

Parameter	Description
up up-value	Set the rising water line for the CPU utilization rate in the range of 1~99.
down down-value	Set the drop water line for CPU utilization, in the range of 1~99.

【Default Configuration】 The default value of CPU waterline is 85% for rising waterline and 75% for falling waterline.

【Command Mode】 Configuration mode

【Default Level】15

【Usage Guide】This command is only available for devices under vsd0, and multiple vsds are not supported.

By setting the maximum CPU usage watermark and turning on monitoring. When the system detects that the CPU usage exceeds the fluctuation range allowed by the maximum waterline, the corresponding Prompt Information will be printed.

【Configuration Example]】1: Set the CPU watermark as the default value, and enable it if monitoring is disabled.

```
AC-FS(config)# default cpu high-watermark set
Reset default cpu watermark monitor
Set system cpu high-watermark up 85%, down 75%
```

2: Turn off CPU watermark monitoring.

```
AC-FS(config)# no cpu high-watermark set
```

```
Close cpu watermark monitor
```

3: Turn on monitoring, the waterline value keeps the value set before turning off.

```
AC-FS(config)# cpu high-watermark set
Open cpu watermark monitor
Set system cpu high-watermark up 85%, down 75%
```

4: Turn on monitoring, and set the rising water line to 90% and the falling water line to 70%.

```
AC-FS(config)#cpu high-watermark set up 90 down 70
Open cpu watermark monitor
Set system cpu high-watermark up 90%, down 70%
```

At this time, the rising waterline of CPU usage is set to 90%, and the falling waterline is set to 70%.

【Verification】-

【Prompt Information】 If the allowable fluctuation range of the CPU usage maximum waterline is 85%~91%, when the CPU usage exceeds the maximum waterline limit, the following alarm information will be printed:

```
*Jan 19 16:23:01: %RG_SYSMON-4-CPU_WATERMARK_HIGH: warning! system cpu usage above high
watermark(91%),current cpu usage 100%
```

When the CPU usage is lower than the lower limit of the maximum watermark, the following alarm information will be printed:

```
*Jan 20 07:02:52:  %RG_SYSMON-5- CPU_WATERMARK:withdraw warning! system cpu usage below high
watermark(85%), current cpu usage 36%
```

【Common Mistake】-

【Platform Description】 -

16.8memory low-watermark set

Configure the memory low watermark threshold and enable detection.

memory low-watermark set mem-value

Disable memory low watermark detection.

no memory low-watermark set

【Parameter Description】

Parameter	Description
mem-value	Memory watermark threshold, the value range is 1~4294967295, the unit is k.

【Default Configuration】 By default, the low memory watermark detection function is disabled.

【Command Mode】 Global mode

【Default Level】-

【Usage Guide】 Enable the low memory watermark detection function and set the memory watermark threshold. When the system memory falls below this threshold, Prompt Information will be printed.

【Configuration Example]】1: Configure the memory low watermark threshold to 500000k, and enable the detection function.

```
AC-FS(config)#memory low-watermark 500000
```

【Verification】-

【Prompt Information】 When the system memory is lower than the set watermark value (for example, set 500000k), the following information will be printed:

```
AC-FS(config)#<187> Jan 1 00:18:59 syslog: Free Memory has dropped below 500000k
```

【Common Mistake】-

【Platform Description】 -

16.9 memory history clear

Clear history entries of memory usage records.

memory history clear [one-forth | half | all]

【Parameter Description】

Parameter	Description
one-forth	Clear a quarter of the entries.
half	Clear out half of the entries.
all	Clear all of the entries.

【Default Configuration】-

【Command Mode】 Global mode

【Default Level】-

【Usage Guide】-

【Configuration Example]】1: Clear half of the history entries of memory usage records.

```
AC-FS# show memory history

Time Thu Jan 1 00:24:45 1970
Used(k) 148516
Maxinum memory users for this period
Process Name  Holding
tcpip.elf 270028 cli-
memory 60600 rg_syslogd
36640

Time Thu Jan 1 00:24:41 1970
Used(k) 148492
Maxinum memory users for this period
Process Name  Holding
tcpip.elf 270028 cli-
memory 52408 rg_syslogd
36640

Time Thu Jan 1 00:24:41 1970
Used(k) 148444
Maxinum memory users for this period
Process Name  Holding
tcpip.elf 270028 cli-
memory 44088 rg_syslogd
36640

AC-FS(config)#memory history clear half
2 out of 5 records in the history table to be cleared...
Clear done !
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

16.10reload

Restart the device.

reload [at { hour [:minute [:second]] } [month [day [year]]]]

【Parameter Description】

Parameter	Parameter
hour [:minute [:second]]	hour [:minute [:second]]
month	month
day	day
year	year

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】-

【Usage Guide】-

【Configuration Example】1: Restart settings.

```
AC-FS#   reload
Reload system?(Y/N) Y
Sending all processes the TERM signal...                    [ OK ]
Sending all processes the KILL signal...                    [ OK ]
Restarting system...
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

16.11 show calendar

Displays the system hardware time.

show calendar

【Parameter Description】-

【Command Mode】 Privileged mode or global mode

【Default Level】-

【Usage Guide】-

【Configuration Example】1: Display the system hardware time.

```
AC-FS# show calendar
21:57:48 GMT Sun, Feb 28, 2012
```

【Prompt Information】-

【Platform Description】 -

16.12 show clock

Displays the system software time.

show clock

【Parameter Description】-

【Command Mode】 Privileged mode or global mode

【Default Level】-

【Usage Guide】-

【Configuration Example】1: When the time zone setting is turned off, the system software time is displayed.

```
AC-FS# show clock
18:22:20 UTC Tue, Dec 11, 2012
```

2: When the time zone setting is turned on, the system software time is displayed.

```
AC-FS# show clock
03:07:49 TSZ Wed, Feb 29, 2012
```

【Prompt Information】-

【Platform Description】 -

16.13 show memory

Displays information about memory.

show memory [sorted total | history | low-watermark | process-id | process-name]

【Parameter Description】

Parameter	Description
sorted total	Sorort by memory usage.
history	Displays a history of the memory usage.
low-watermark	Displays the system memory low waterline value.
process-id	Displays the memory usage for the specific task specified by the process-id.
process-name	Displays the memory usage for the specific task specified by the process-name.

【Command Mode】 Privileged mode or global mode

【Default Level】-

【Usage Guide】Each time show memory history is executed, one more entry will be displayed, and a maximum of 10 entries will be displayed. You can use the memory history clear command to clear the history entries.

【Configuration Example]】1: Display the current memory usage of each task and sort by total size.

```
AC-FS# show memory sorted
System Memory: 508324K total, 481560K used, 26764K free, 31.5% used rate
Used detail:   149112K active, 247776K inactive, 30460K mapped, 50460K slab, 3752K others

PID      Text(K) Rss(K)  Data(K)         Stack(K) Total(K)        Process
807      1568    4584    264728          84       270028          tcpip.elf
854      40      1436    246076          84       248840          cli-filesystem
1237     52      1492    123260          84       126036          cli-memory
803      56      1104    74064           84       76920           ping.elf
727      84      1276    33812           84       36640           rg_syslogd
733      84      796     33536           84       36364           rg_syslogd
776      224     1416    16896           84       19800           lsmdemo
858      40      1324    16844           84       19612           rg-tty-admin
769      40      3600    11052           84       13812           skbdemo
--More--
```

Description table of some keyword information displayed by this command:

keywords	Description
total	total system memory
used	used memory
free	remaining memory
used rate	memory usage percentage
Active	active page
inactive	inactive page
mapped	mapped memory
slab	Memory consumed by slab
others	The amount of memory in Used except active, inactive, mapped, slab

Description table of displayed information for each current task:

Field	Description
PID	Process ID.
Text	Snippet size.
Rss	resident memory size.
Data	data segment size.
Stack	stack size.
Total	total memory consumption.
Process	task name.

【Prompt Information】-

【Platform Description】 -

16.14 show memory vsd

Displays information about memory.

show memory vsd vsd_id

【Parameter Description】

Parameter	Description
vsd_id	The number of the vsd you want to see is a number, you can find the vsd id number of each vsd from show vsd. The value range is [0, 16].

【Command Mode】 Privileged mode or global mode

【Default Level】-

【Usage Guide】Only the device has the command under vsd0.

【Configuration Example]】1: Display the memory usage of each task under vsd 1.

```
AC-FS#show memory vsd 1
PID     Text    Rss     Data    Stack   Total   Process
1408    244     1192    25400   84      32164   tty_secu_enable
1385    104     16288   648     84      18648   gvpd
1384    304     3872    17084   84      24728   wbamain
1382    376     17708   33656   84      53308   snooping.elf
1381    84      2156    16736   84      22956   password_policy
1380    72      1096    404     84      3848    dns_client.elf
1379    168     2580    472     84      5352    rg-rmond
1378    652     3504    9768    84      15964   rg-snmpd
1376    208     1452    10672   84      14872   rg-fsui
1375    116     2020    33464   84      37288   rg-telnetc
1373    24      844     220     84      2824    rg-telnetd
1372    724     2364    17016   84      24380   rg-sshd
1371    244     2996    35780   84      42544   rg-tty-admin
1365    132     2168    9004    84      13796   vrrp_plus.elf
1364    312     16944   764     84      20368   vrrp.elf
1363    124     16988   500     84      19744   lacp.elf
1358    24      1380    320     84      3536    ftpc_cli.elf
1357    124     1944    8552    84      14976   ftp_server.elf
1352    340     3032    74704   84      80768   dhcp6.elf
1351    312     1960    988     84      6116    dhcp.elf
1350    388     17808   920     84      21600   mstp.elf
1349    240     3876    976     84      9536    rpi.elf
1348    1316    4656    1004    84      10764   isis.elf
1347    212     4220    872     84      9368    ripng.elf
1345    460     4284    876     84      9656    rip.elf
1344    1800    5568    1572    84      12156   bgp.elf
1340    1084    4700    1024    84      10928   ldp.elf
1339    288     17684   556     84      21472   msf.elf
1338    208     3604    42712   84      47708   rg-syslogd
--More--
```

【Prompt Information】-

【Platform Description】 -

16.15show pci-bus

Displays information about devices attached to the PCI bus.

show pci-bus

【Parameter Description】-

【Command Mode】 Privileged mode or global mode

【Default Level】-

【Usage Guide】-

【Configuration Example】1: Display the information about the device hanging on the PCI bus.

```
AC-FS# show pci-bus
NO:0
Vendor ID             :  0x1131
Device ID             : 0x1561
Domain:bus:dev.func : 0000:00:05.0
Status / Command      : 0x2100000
Class / Revision      : 0xc031030
Latency               : 0x0
first 64 bytes of configuration address space:
00: 31 11 61 15 00 00 10 02 30 10 03 0c 20 00 80 00
10: 00 00 00 f0 00 00 00 00 00 00 00 00 00 00 00 00
20: 00 00 00 00 00 00 00 00 00 00 00 00 31 11 61 15
30: 00 00 00 00 dc 00 00 00 00 00 00 00 29 01 01 2a
  NO:1
Vendor ID             :  0x1131
Device ID             : 0x1562
Domain:bus:dev.func : 0000:00:05.1
Status / Command      : 0x2100156
Class / Revision      : 0xc032030
Latency               : 0x30
First 64 bytes of configuration address space:
00: 31 11 62 15 56 01 10 02 30 20 03 0c 20 30 80 00
10: 00 10 00 f0 00 00 00 00 00 00 00 00 00 00 00 00
20: 00 00 00 00 00 00 00 00 00 00 00 00 31 11 62 15
30: 00 00 00 00 dc 00 00 00 00 00 00 00 29 01 02 10
```

【Prompt Information】-

【Platform Description】 -

16.16 show processes cpu

Display system task information.

show processes cpu [history [table] | [5sec | 1min | 5min | 15min] [nonzero]]

【Parameter Description】

Parameter	Description
5sec | 1min | 5min | 15min	Descending order of CPU utilization over the last 5 seconds, 1 minute, 5 minutes, 15 minutes.
Nonzero	Arranged list of task information.
History	Do not display information for tasks with zero CPU utilization.
Table	In the form of a histogram, the time periods of the past 60 seconds, 60 minutes, and 72 hours are displayed

【Command Mode】 Privileged mode or global mode

【Default Level】-

【Usage Guide】This command is only available for devices under vsd0, and multiple vsds are not supported.

【Configuration Example]】1: Task information sorted in ascending order by the ID numbers of all tasks in the system

```
AC-FS# show processes cpu
System Uptime: 19:08.6
CPU utilization for five seconds:1.2%; one minute:0.8%; five minutes:0.8%
set system cpu watermark (open): high 80%(85%~75%)

Tasks Statistics: 375 total, 10 running, 365 sleeping, 0 stopped, 0 zombie
  Pid Vsd S   PRI  P       5Sec       1Min       5Min      15Min Process
    1   0 S    20  0   0.0(0.0)   0.0(0.0)   0.0(0.0).....0.0(0.0) init
    2   0 S    20  1   0.0(0.0)   0.0(0.0)   0.0(0.0).....0.0(0.0) kthreadd
    3   0 S  -100  0   0.0(0.0)   0.0(0.0)   0.0(0.0).....0.0(0.0) migration/0
    4   0 S    20  0   0.0(0.0)   0.0(0.0)   0.0(0.0).....0.0(0.0) ksoftirqd/0
    5   0 S  -100  1   0.0(0.0)   0.0(0.0)   0.0(0.0).....0.0(0.0) migration/1

 --More--
```

2: Sort in ascending order by the ID numbers of all tasks in the system, and do not display the information of tasks whose CPU utilization is 0 within 15 minutes.

```
AC-FS# show processes cpu nonzero
```

The command displays the information Description table shown at the beginning:

Field Description:

Field	Description
System Uptime	The total running time of the device, accurate to the second.
CPU Utilization	The last 5 seconds, 1 minute, 5 minutes to control the total CPU utilization of the core.
Virtual CPU usage	On the virtual core, the last 5 seconds, 1 minute, 5 minutes control the total CPU utilization of the core.
Tasks Statistics	Task statistics, statistics of the total number of tasks and task status.
set system cpu watermark	Control the total cpu watermark setting value and state of the core.

The running status of tasks in the system is as follows:

Task Running Status Meter	Description
running	running task.
sleeping	pending tasks.
stopped	suspended task.
zombie	Tasks terminated and not recycled by the system.

Information Description table of each displayed task:

Field	Description
Pid	task ID number
Vsd	own vsd number
S	Task state, a total of 5 kinds, R(running), T(stopped), S(sleeping), D(waiting), Z(zombie)
PRI	task run priority
P	Which cpu core the task is running on
5sec/1min/5min/15min	The CPU usage of the task over the past 5 seconds, 1 minute, 5 minutes, 15 minutes. The value in parentheses is the cpu utilization not divided by the total number of cores that the task is currently on.

Process	mission name Only the first 15 characters are displayed at most, any characters beyond that will be truncated

3: Sort in ascending order by task ID number, and only display thread information with non-zero CPU utilization within 15 minutes.

```
AC-FS #show processes cpu nonzero
```

4: Sort in descending order of CPU utilization within 5 seconds, and do not display task information with zero CPU utilization within 1sec.

```
AC-FS #show processes cpu 5sec nonzero
```

5: Display the system's control core cpu utilization in the form of a histogram, and the usage information in the past 60 seconds, 60 minutes, and 72 hours. Among them, the first chart is the CPU utilization of the control core of the system within 300 seconds. Each small grid on the abscissa is 5 seconds, and each grid on the ordinate is 5%. value, that is, the first cell on the abscissa closest to 0 is the cpu utilization value in the last 5 seconds, the unit is %.

The second chart is the CPU utilization value of the control core of the system in the last 60 minutes, the unit is %, and each cell on the abscissa is 1 minute. The third chart is the CPU utilization value of the control core of the system in the last 72 hours, the unit is %, and each cell on the abscissa is 1 hour. An example is as follows:

```
AC-FS#show processes cpu history

             system cpu percent usage(%) [last 300 second]
    _
```

```
100|
 95|
 90|
 85|
 80|
 75|
 70|
 65|
 60|
 55|
 50|
 45|
 40|*********
 35|||||||||||
 30|||||||||||*
 25||||||||||||
 20||||||||||||
 15||||||||||||
 10||||||||||||
  5||||||||||||***************
  0|||||||||||||||||||||||||||
   #=========#=========#=====*=>
   0         50        100       second
       system cpu percent usage(%) per 5second (last 125 second)
```

```
           system cpu percent usage(%) [last 60 minute]
   -
100|
 95|
 90|
 85|
 80|
 75|
 70|
 65|
 60|
 55|
 50|
 45|
```

```
 40|
 35|
 30|*
 25||
 20||
 15||
 10||
  5||*
  0|||
   #==*==>
   0     minute
       system cpu percent usage(%) per 1minute (last 2 minute)
```

6: Display the system cpu (0 core) usage information in the past 60 seconds, 60 minutes and 72 hours in a tabular manner.

Among them, the first large table is the cpu utilization of the system within 300 seconds, the first grid is the value of the cpu utilization in the last 5 seconds, the unit is %, and the interval of each small grid is 5 seconds.

The second large table is the cpu utilization value of the last 60 minutes, the unit is %, and the interval of each small grid is 1 minute. The third large table is the cpu utilization value of the last 72 hours, the unit is %, and the interval of each small grid is 1 hour. Examples are as follows:

```
AC-FS #show processes cpu history table
             system cpu percent usage(%) [last 300 second]
#-------------------------------------------------------------------------------#
|        |    1|    2|    3|    4|    5|    6|    7|    8|    9|   10|
#-------------------------------------------------------------------------------#
#-------------------------------------------------------------------------------#
|      0|  2.0|  2.4|  2.3|  2.3|  2.8|  3.0|  2.7|  3.2|  2.6|  2.4|
#-------------------------------------------------------------------------------#
|      1|  2.7|  2.5|  2.7|  2.2|  2.4|  2.6|  2.2|  2.7|  2.3|  2.5|
#-------------------------------------------------------------------------------#
|      2|  2.9|  2.0|  2.4|  2.5|  2.7|  2.4|  2.4|  2.6|  2.6|  2.5|
#-------------------------------------------------------------------------------#
|      3|  2.7|  2.8|  2.8|  3.2|  2.5|  3.2|  3.1|  4.0|  2.7|  2.7|
#-------------------------------------------------------------------------------#
|      4|  4.0|  2.3|  2.1|  2.2|  2.7|  2.4|  2.5|  2.6|  2.4|  2.6|
#-------------------------------------------------------------------------------#
|      5|  2.4|  3.2|  2.5|  2.3|  2.3|  3.6|  2.8|  2.5|  2.2|  2.4|
#-------------------------------------------------------------------------------#

             system cpu percent usage(%) [last 60 minute]
#-------------------------------------------------------------------------------#
|        |    1|    2|    3|    4|    5|    6|    7|    8|    9|   10|
```

```
#-------------------------------------------------------------------------------#
#-------------------------------------------------------------------------------#
|      0|  2.6|  2.5|  3.0|  2.4|  2.6|
#-------------------------------------------------------------------------------#
```

【Prompt Information】-

【Platform Description】 -

16.17 show processes cpu detailed

Displays detailed information about the specified task.

show processes cpu detailed { process-id | process-name }

【Parameter Description】

Parameter	Description
process-id	View the task information of the specified task ID number.
process-name	View the task information of the specified task name.

【Command Mode】 Privileged mode or global mode

【Default Level】 -

【Usage Guide】 This command is only available for devices under vsd0, and multiple vsds are not supported.

【Configuration Example]】 1: View the task information of the specified task name.

```
AC-FS# show processes cpu detailed demo
Process Id  : 1820
Process Name : demo
Vsdid       : 0
Process Ppid  : 1

State         : R(running)
On CPU        :   0
Priority : 20
Age Time       : 24:06.5
Run Time       : 00:01.0
Cpu Usage  :
    Lass  5 sec.....0.3% (0.6%)
    Lass  1 min.....0.3% (0.6%)
    Lass  5 min.....0.3% (0.6%)
    Lass 15 min.....0.3% (0.6%)
```

```
Tty           : ?
```

Code Usage: 209.6KB. If the specified task name is not unique, it is as follows:

Display information Description table:

Field Description:

Field	Description
Process Id	task ID number.
Vsdid	The vsd number to which the task belongs.
Process Name	mission name.
Process Ppid	The ID number of the parent process task.

State	task running status.
On CPU	The CPU the task is running on.
Priority	task priority.
Age Time	The duration of the task since it was started.
Run Time	The time from when the task was started to when it was scheduled for execution.
Cpu Usage	The task's CPU usage over the past 5 seconds, 1 minute, 5 minutes, 15 minutes. The value in parentheses is the cpu utilization not divided by the total number of cores that the task is currently on. For example, the demo task is currently on core 0, core 0 is the control core, and the system has a total of two control cores, it shows 0.3% (0.6%).
Tty	Tty number. "Major Device Number, Minor Device Number", if 0 is "?".
Code Usage	The size occupied by the task code segment.

2: View the task information of the specified task ID.

```
AC-FS# show process cpu detailed 1715
```

【Prompt Information】-

【Platform Description】 -

16.18 show processes vsd

Press vsd to display system task information.

show process vsd vsd_id cpu

【Parameter Description】

Field	Description
vsd_id	The number of the vsd you want to see is a number that can be found from show vsd for each vsd id number of each vsd from show vsd. The range of values is [0, 16].

【Command Mode】 Privileged mode or global mode

【Default Level】-

【Usage Guide】Only devices under vsd0 have this command, and multiple vsds are not supported.

【Configuration Example]】1: Display system task information under vsd1

```
AC-FS#show processes vsd 1 cpu
```

【Prompt Information】-

【Platform Description】 -

16.19show usb-bus

Displays information about devices attached to the USB bus.

show usb-bus

【Parameter Description】-

【Command Mode】 Privileged mode or global mode

【Default Level】-

【Usage Guide】-

【Configuration Example】1: Display the information about the device hanging on the USB bus.

```
AC-FS# show usb-bus
Device: Linux Foundation 2.0 root hub
  Bus 001 Device 001: ID 1d6b:0002
```

【Prompt Information】-

【Platform Description】 -

16.20show version

Display system version information.

show version

【Parameter Description】-

【Command Mode】 Privileged mode or global mode

【Default Level】-

【Usage Guide】-

【Configuration Example】1: Display system version information.

```
AC-FS# show version
System description      : AC-FS Indoor AP320-I (802.11a/n and 802.11b/g/n) By AC-FS Networks
System start time       : 2012-12-06 00:00:00
System uptime           : 0:03:20:07
System hardware version : 1.0.0
System software version : AP_RGOS11.0(1B1)
System serial number : 1234942570018
System boot version  : 1.0.0
```

【Prompt Information】-

【Platform Description】 -

16.21 show cpu

Displays information about system tasks on the control core and not on the virtual core.

show cpu

【Parameter Description】-

【Command Mode】 Privileged mode or global mode

【Default Level】-

【Usage Guide】This command is only available for devices under vsd0, and multiple vsds are not supported.

If there are virtual cores in the system, you need to view the cpu utilization information of the virtual cores, see the related commands of show processes cpu.

【Configuration Example】1: Display the information of system tasks on the control core and not on the virtual core.

```
AC-FS#show cpu
=============================================
CPU Using Rate Information
CPU utilization in five seconds: 4.80%
CPU utilization in one minute:  4.10%
CPU utilization in five minutes:  4.00%

 NO      5Sec     1Min     5Min Process
    1   0.00%    0.00%.....0.00% init
    2   0.00%    0.00%.....0.00% kthreadd
    3   0.00%    0.00%.....0.00% ksoftirqd/0
    4   0.00%    0.00%.....0.00% events/0
--More--
```

【Prompt Information】-

【Platform Description】 -

16.22 show reboot-reason

Displays the reason for the restart of the device.

show reboot-reason

【Parameter Description】-

【Command Mode】 User mode, privileged mode, global mode

【Default Level】1

【Usage Guide】-

【Configuration Example】1: Only the reason for restarting the device is displayed.

```
AC-FS#show reboot-reason
time: 1970-01-01 08:03:13
reason: reload cmd
info: /sbin/rg-sysmon/3844
  AC-FS#
```

【Prompt Information】-

【Platform Description】 -

17 NTP

17.1no ntp

Turn off the NTP synchronization service, stop synchronization with the time server, and clear all NTP configuration information.

no ntp

【Parameter Description】-

【Default Configuration】 By default, the NTP service is disabled.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 By default, the NTP function is disabled, but as long as the NTP server or the NTP security identification mechanism is configured, the NTP function will be enabled.

【Configuration Example】1: Disable the NTP service.

```
AC-FS(config)# no ntp
```

【Verification】show run to check whether there is still NTP configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.2ntp access-group

Configure access control permissions for the NTP service.

ntp access-group { peer | serve | serve-only | query-only } access-list-number | access-list-name

Unset access control permissions.

no ntp access-group {peer | serve | serve-only | query-only} access-list-number | access-list-name

【Parameter Description】

Parameter	Description
peer	Allows both time requests and control queries to the local NTP service, and allows the local device to synchronize time with remote systems (full access).
serve	Allows time requests and control queries to the local NTP service, but does not allow the local device to synchronize time with the remote system.
serve-only	Time requests are only allowed to the local NTP service.
query-only	Only control queries to the local NTP service are allowed.
access-list-number	IP access control list number; the range is 1 to 99 and 1300 to 1999.
access-list-name	IP access control list name.

【Default Configuration】 By default, no NTP access control rules are configured.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】Set the access control permission to the local device NTP service. A minimal security measure is provided here, a more secure approach is to use the NTP authentication mechanism.

When an access request arrives, the NTP service matches the rules in order from the smallest access limit to the largest access limit, and the first matched rule shall prevail. The matching order is peer, serve, serve-only, query-only.

If no access control rules are configured, all access is allowed. But once an access control rule is configured, only the access allowed in the rule can take place.

Currently the system does not support the control query function. Although the rules are matched in the above order, requests related to control queries cannot be supported.

【Configuration Example]】1: The configuration only allows the device of 192.168.1.1 to make time requests to the local device

```
AC-FS(config)# access-list 1 permit 192.168.1.1
AC-FS(config)# ntp access-group serve-only 1
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.3ntp authenticate

Configure the NTP service to use the NTP global authentication mechanism.

ntp authenticate

Turn off the global security identification mechanism.

no ntp authenticate

【Parameter Description】-

【Default Configuration】 By default, the NTP global authentication mechanism is disabled.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 If the global security identification mechanism is not used, the synchronous communication will not be encrypted. Only when the global security identification mechanism is turned on and other global key configurations are completed, it is possible to initiate encrypted communication with the server.

The verification standard is the trust key specified by ntp authentication-key and ntp trusted-key.

【Configuration Example]】1: After configuring the corresponding global authentication key and specifying it as the global trust key, open the authentication mechanism.

```
AC-FS(config)# ntp authentication-key 6 md5 wooooop AC-
FS(config)# ntp trusted-key 6
AC-FS(config)# ntp authenticate
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.4ntp authentication-key

Configure a global NTP authentication key for the NTP service.

ntp authentication-key key-id md5 key-string [enc-type]

Cancel the global NTP authentication key.

no ntp authentication-key key-id

【Parameter Description】

Parameter	Description
key-id	Key ID; The value range is 1 ~ 4294967295.
key-string	Key string.
enc-type	(Optional) whether the key is encrypted. 0 means no encryption and 7 means simple encryption. The default is no encryption

【Default Configuration】 By default, no authentication key is configured.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Configure the global authentication key and use md5 for encryption. Each key has a unique key-id identifier. Customers can use ntp trusted-key to set the key corresponding to the key-id as the global trusted key.

There is a limit of 1024 keys, but only one key per server is supported.

【Configuration Example]】 1: Configure an authentication key with ID 6:

```
AC-FS(config)# ntp authentication-key 6 md5 wooooop
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

17.5ntp disable

Disable the function of receiving NTP packets on the corresponding interface.

ntp disable

【Parameter Description】-

【Default Configuration】 By default, all interfaces can accept NTP packets.

【Command Mode】 Interface configuration mode

【Default Level】-

【Usage Guide】 By default, the NTP packets received on any interface can be provided to the client for clock adjustment. By setting this function, the NTP packets received on the corresponding interface can be blocked.

The interface that can perform this configuration must be the interface that can configure IP to send and receive packets, and this command does not exist on other interfaces.

【Configuration Example】1: Disable the interface to receive NTP packets:

```
AC-FS(config-if)# no ntp disable
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.6ntp interval

Set the time interval that the NTP Client needs to synchronize the clock with the NTP Server regularly.

ntp interval seconds

Cancel the NTP synchronization interval setting and restore to the default synchronization interval.

no ntp interval

【Parameter Description】

Parameter	Description
seconds	Interval of timing synchronization, in seconds. The value range is 10 ~ 2592000 (s), and the default value is 64S。

【Default Configuration】 64s

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 ≒ The time interval set here will not take effect immediately. If you want to take effect immediately, please enable NTP and configure the time interval. If NTP has not successfully synchronized the time, it will quickly synchronize the time at intervals of 5s. After the time synchronization is successful, the time will be synchronized at the set time interval.

【Configuration Example]】1: Configure NTP to synchronize time every hour

```
AC-FS(config)# ntp interval 3600
```

【Verification】1: Use the show run command to view NTP related parameters.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 This command is only supported on some versions.

17.7ntp master

Set the local clock as the NTP master clock (the local clock reference source is reliable) to provide synchronized time for other devices.

ntp master [stratum]

Cancel the NTP master clock setting.

no ntp master

【Parameter Description】

Parameter	Description
stratum	(Optional) Specify the number of layers the local clock is on, in the range of 1 to 15; the default value is 8 if the Parameter is not specified.

【Default Configuration】 The NTP master clock function is not configured by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Under normal circumstances, the local system will be directly or indirectly synchronized with the external clock source. However, if the local system cannot be synchronized with the external clock source due to network connection failure or other reasons, you can use this command to set the local clock reference source to be reliable and provide synchronization time for other devices.

Once this is set, the system will not synchronize to a clock source with a higher number of clock tiers than its own.

Special care must be taken when using this command. Setting the local clock to the master clock (especially if a lower clock tier value is specified) is likely to overwrite the real valid clock source. If this command is used on multiple devices in the same network, the clock synchronization of the network may be unstable due to clock differences between the devices.

If the system has never been synchronized with an external clock source before using this command, it may be necessary to manually calibrate the system clock to ensure that it does not deviate too much.

【Configuration Example]】1: Set the local clock reference source to be reliable, and set the number of clock layers to 12.

```
AC-FS(config)# ntp master 12
```

【Verification】1: Use the show ntp status command to view the NTP related configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.8ntp server

Specify an NTP server for the NTP client.

ntp server { ip-addr | domain | ip domain | ipv6 domain } [version version] [source if-name] [key keyid] [prefer]

Delete the specified NTP server.

no ntp server ip-addr

【Parameter Description】

Parameter	Description
ip-addr	Set the IP address of the NTP server, supporting IPv4 and IPv6.
domain	Set the domain name of the NTP server, supporting IPv4 and IPv6.
version	(optional) specify the version of NTP (1-3). Ntpv3 version is adopted by default.
if-name	(optional) specify the source interface (layer-3 interface) for sending NTP message. By default, it is routed according to the device.
keyid	(optional) specifies the encryption key used to communicate with the corresponding server. It is not encrypted by default. Value range 1~4294967295.
prefer	(optional) specify the corresponding server as the system preference server, which is not the preference server by default.

【Default Configuration】 The NTP server is not configured by default.

【Command Mode】 Global configuration mode.

【Default Level】 14

【Usage Guide】 Currently, FS FSOS system only supports clients but not servers, and supports a maximum of 20 synchronization servers. To perform encrypted communication with the server, you first need to set the global encryption key and the global trust key, and then specify the corresponding key as the server trust key before you can initiate encrypted communication with the server. To complete the encrypted communication requirements with the server The server has the same global encryption key and global trust key

Under the same situation (accuracy), prefer the clock for synchronization

When configuring the source interface for NTP to send packets, you should pay attention. The configured interface must be an interface configured with IP and can communicate with the corresponding NTP server.

【Configuration Example】 1: Configure the device on the network as the NTP server.

```
AC-FS(config)# ntp server 192.168.210.222 //IPv4 configure
AC-FS(config)# ntp server 10::2 // IPv6 configure
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】-

17.9ntp service disable

Disable NTP to provide time synchronization services to the outside world.

ntp service disable

Enable NTP to provide external time synchronization services.

no ntp service disable

【Parameter Description】-

【Default Configuration】 The default NTP can provide time synchronization service.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 NTP is in client/server mode. After the device successfully synchronizes time from an external reliable clock source, it will serve as a time synchronization server to provide external time synchronization services. If you only want to use NTP only as a client, you need to configure this command to disable the time synchronization service provided by NTP.

This command and the ntp master function are mutually exclusive. When the ntp master function is enabled, the device as a server cannot disable the external time synchronization service function. If this command is configured, the ntp master function cannot be enabled.

【Configuration Example】1: Disable the time synchronization function provided by NTP.

```
AC-FS(config)# ntp service disable
```

【Verification】1: Use the show run | in ntp command to view the NTP related configuration.

【Prompt Information】

【Common Mistake】

【Platform Description】 This command is only supported on some versions.

17.10ntp trusted-key

Configure a key corresponding to an ID as a global trust key.

ntp trusted-key key-id

Delete the global trust key corresponding to the ID.

no ntp trusted-key key-id

【Parameter Description】

Parameter	Description
key-id	Global trust key ID. Value range: 1~4294967295.

【Default Configuration】 There is no trust key by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 In NTP communication, both parties must use the same trust key. The key is searched by ID, and the key itself is not transmitted to improve security.

【Configuration Example]】 1: Configure an authentication key and set this key as the corresponding server trust key.

```
AC-FS(config)# ntp authentication-key 6 md5 wooooop AC-
FS(config)# ntp trusted-key 6
AC-FS(config)# ntp server 192.168.210.222 key 6
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

17.11ntp update-calendar

Set up an NTP client to periodically update the device's hardware clock with a clock value synchronized from an external clock source.

ntp update-calendar

Cancel the periodic update of the hardware clock function.

no ntp update-calendar

【Parameter Description】-

【Default Configuration】 The function of regularly updating the hardware clock is not configured by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this function to allow the NTP client to periodically update the hardware clock of the device with the clock value synchronized from the external clock source. The device's hardware clock continues to run even when the device is powered off or the device is reset.

By default, NTP is not configured to update the hardware clock. Once configured, the NTP client will also update the device's hardware clock every time it successfully synchronizes with an external clock source.

【Configuration Example】1: Configure NTP to update the hardware clock regularly.

```
AC-FS(config)# ntp update-calendar
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

17.12 show ntp server

Displays NTP server information.

show ntp server

【Parameter Description】-

【Command Mode】 Privileged user mode, global configuration mode, interface configuration mode, VLAN configuration mode.

【Default Level】 14

【Usage Guide】 If the NTP service is configured, the current NTP server information will be displayed, otherwise this command will not print any information.

【Configuration Example】1: Display the NTP server information of the current system

```
AC-FS# show ntp server
```

```
ntp-server                                source    keyid        prefer  version
----------------------------------------  --------  -----------  ------  -------
10::2                                     None      None         FALSE   3
192.168.210.222                           None      None         FALSE   3
```

Field Description:

Field	Description
ntp-server	Indicates the IP address or domain name of the NTP server.
source	Indicates the source port of the NTP server.
keyid	Indicates whether the encryption key is used for communication with the corresponding server.
prefer	Indicates whether the corresponding server is a system prefer server.
version	Indicates the version of NTP (1-3).

【Prompt Information】-

【Platform Description】 -

17.13 show ntp status

Display NTP information.

show ntp status

【Parameter Description】

【Command Mode】 Privileged user mode, global configuration mode, interface configuration mode, VLAN configuration mode.

【Default Level】 14

【Usage Guide】 If the NTP service of the system is turned on, the current NTP information will be displayed. This command will not print any information until the synchronization server is added for the first time.

【Configuration Example】1: Display the NTP information of the current system

```
AC-FS# show ntp status
Clock is synchronized, stratum 8, reference is 127.127.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24
reference time is D4BD819B.433892EE (01:27:55.000 UTC )
clock offset is 0.00000 sec, root delay is 0.00000 sec
root dispersion is 0.00002 msec, peer dispersion is 0.00002 msec
```

Field Description:

Fields	Description
stratum	Indicates the current clock level.
reference	Indicates the address of the synchronization server.
freq	Indicates the current system clock frequency.
precision	Indicates the current system clock accuracy.
reference time	Indicates the UTC time value of the synchronization server reference clock.
clock offset	Indicates the current clock offset.
root delay	Indicates the current clock delay.
root dispersion	Indicates top server time accuracy.
peer dispersion	Indicates the synchronization server time accuracy.

【Prompt Information】-

【Platform Description】 -

18 SNTP

18.1sntp enable

Set to enable the SNTP function.

sntp enable

Return this setting to the default value—Disable.

no sntp enable

【Parameter Description】-

【Default Configuration】 The default SNTP state is Disable.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: Enable SNTP function.

```
AC-FS(config)# sntp enable
```

【Verification】1: Use the show sntp command to view SNTP related parameters.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

18.2sntp interval

Set the time interval that the SNTP Client needs to synchronize the clock with the NTP/SNTP Server.

sntp interval seconds

Cancel the SNTP synchronization interval setting and restore to the default synchronization interval.

no sntp interval

【Parameter Description】

Parameter	Description
seconds	The interval of timing synchronization in seconds. Value range 60 to 65535.

【Default Configuration】 1800s

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 The time interval set here will not take effect immediately. If you want to take effect immediately, please execute the sntp enable command after configuring the time interval.

【Configuration Example]】1: Configure SNTP to synchronize time every hour

```
AC-FS(config)# sntp interval 3600
```

【Verification】1: Use the show sntp command to view SNTP related parameters.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

18.3 sntp server

Set up SNTP Server.

sntp server ip-address

Delete the specified SNTP/NTP Server

no sntp server

【Parameter Description】

Parameter	Description
ip-address	IP address of the NTP/SNTP server

【Default Configuration】 No NTP/SNTP server is set by default

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Since the SNTP protocol is fully compatible with NTP, the set SNTP Server can be completely configured as a public NTP Server on the internet.

【Configuration Example】1: Configure the NTP server on the network

```
AC-FS(config)# sntp server 192.168.4.12
```

【Verification】1: Use the show sntp command to view SNTP related parameters.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

18.4 show sntp

Display the related parameters of SNTP.

show sntp

【Parameter Description】-

【Command Mode】 Privileged user mode, global configuration mode, interface configuration mode

【Default Level】 14

【Usage Guide】-

【Configuration Example】1: View the related parameters of SNTP.

```
AC-FS# show  sntp
SNTP state             : Enable
SNTP server.....192.168.4.12
SNTP sync interval   : 60
Time zone              : +8
```

Field Description:

Field	Description
state	Indicates that sntp is enabled
server	Represents a time synchronization server
sync interval	Indicates the time synchronization interval
Time zone	current time zone

【Prompt Information】-

【Platform Description】 -

19 TIME RANGE

19.1absolute

Set the absolute time interval.

absolute { [start time date] [end time date] }

Delete an existing absolute time interval.

no absolute

【Parameter Description】

Parameter	Description
start time date	Start time of interval.
end time date	End time of interval.

【Default Configuration】 There is no absolute time interval configured.

【Command Mode】 time-range mode

【Default Level】 14

【Usage Guide】 If you want a function to take effect in an absolute time interval, you can use the absolute command to configure a start and end time interval.

【Configuration Example]】1: Create a time range and enter time range mode.

```
AC-FS(config)# time-range no-http
AC-FS(config-time-range)#
```

2: Configure the absolute time interval.

```
AC-FS(config-time-range)# absolute start 1:1 1 JAN 2013 end 1:1 1 JAN 2014
```

【Verification】1: Use the show time-range [time-range-name] command to view the configuration of the time range.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

19.2periodic

Set the cycle time.

periodic day-of-the-week time to [day-of-the-week] time

Delete an existing cycle time.

no periodic day-of-the-week time to [day-of-the-week] time

【Parameter Description】

Parameter	Description
day-of-the-week	The cycle time starts or ends on the day of the week.
time	What time of day does the cycle time start or end?

【Default Configuration】 No cycle time is configured

【Command Mode】 time-range mode

【Default Level】 14

【Usage Guide】If you want a function to take effect within a period, you can use the periodic command to configure a period.

【Configuration Example]】1: Create a time range and enter time range mode

```
AC-FS(config)# time-range no-http
AC-FS(config-time-range)#
```

2: Configure the absolute time interval

```
AC-FS(config-time-range)# periodic Monday 1:1 to Tuesday 2:2
```

【Verification】1: Use the show time-range [time-range-name] command to view the configuration of the time range.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

19.3 show time-range

Display time range information.

show time-range [time-range-name]

【Parameter Description】

Parameter	Description
time-range-name	You can specify to display information about a time range.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 You can use this command to verify whether the configured time range is correct.

【Configuration Example】1: Display time range information.

```
AC-FS# show time-range
time-range entry: test (inactive)
  absolute end 01:02 02 February 2012
```

【Prompt Information】-

【Platform Description】 -

19.4time-range

Create a time range and enter the time range configuration mode.

time-range time-range-name

Delete an existing time range.

no time-range time-range-name

【Parameter Description】

Parameter	Description
time-range-name	The name of the time range to create.

【Default Configuration】 No time range is configured

【Command Mode】 Global mode

【Default Level】 2

【Usage Guide】 Some applications (such as ACL) may run based on time, such as making ACL take effect during certain time periods of a week, etc. In order to achieve this requirement, a time range must be configured first. After the time range is created, the corresponding time control can be configured in the time range mode.

【Configuration Example]】1: Create a time range

```
AC-FS(config)# time-range no-http
AC-FS(config-time-range)#
```

【Verification】1: Use the show time-range [time-range-name] command to check whether the time range exists.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

20 Abnormal alarm

20.1feedback frequency

Configure email sending frequency

feedback frequency min

Restore Default Configuration

no feedback frequency

【Parameter Description】

Parameter	Description
frequency min	Transmission frequency. The unit is minutes, and the default is 60. Configurable range: 5-10080.

【Default Configuration】 60

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】If you want to receive emails as soon as possible when there is an abnormality, the value should be as small as possible; the smaller the value, the more timely you can receive abnormal alarm emails. However, if there is a lot of abnormal information, you will receive emails frequently.

If you don't want to receive emails frequently, you can set the value to a larger value, such as one day. Then, for abnormal information within a day, only one email is sent, and it is very likely that the email cannot be received immediately after the exception occurs.

Please set the email sending frequency according to your needs.

【Configuration Example】1: Set the email sending frequency to 2 hours.

```
AC-FS(config)# feedback frequency 120
```

【Verification】1: Use the show run command to view the configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

20.2feedback ignore item

Set ignored alert option id.

feedback ignore-item item-id

Delete configuration.

no feedback ignore-item item-id

【Parameter Description】

Parameter	Description
ignore-item item-id	Set the ignored option id. range 0-8.

【Default Configuration】-

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】After configuring ignore, this item will not send email even if it is abnormal.

【Configuration Example】1: Set the email sending frequency to 2 hours.

```
AC-FS(config)# feedback frequency 120
```

【Verification】1: Use the show run command to view the configuration.

【Prompt Information】 If the configured id exceeds the range, it prompts that the command input is incorrect.

【Common Mistake】 The configured id is not supported, and it prompts that the command input is incorrect.

【Platform Description】 -

20.3feedback subscriber

Set the email address to receive messages.

feedback subscriber mail-addr

Delete configuration.

no feedback subscriber mail-addr

【Parameter Description】

Parameter	Description
subscriber mail-addr	Set the email address to receive messages. Can be configured multiple times, supports up to 6.

【Default Configuration】-

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 If you need to send to multiple people's mailboxes, execute this command repeatedly.

【Configuration Example】1: Set recipients.

```
AC-FS(config)# feedback subscriber AC-FS@sina.com.cn
```

【Verification】1: Use the show run command to view the configuration.

【Prompt Information】-

【Common Mistake】 The configured email address is unreachable. The command does not check for format and reachability, and needs to be checked by the user.

【Platform Description】 -

20.4feedback user enable

Enable the abnormal alarm function.

feedback user enable

Disable abnormal alarm function

no feedback user enable

【Parameter Description】-

【Default Configuration】Close

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 To use the abnormal alarm function, you must enable it.

The following functions need to be configured at the same time for normal use:

1. Open the mail service

2. Configure smtp server

3. Configure the account and password to send

4. Configure recipient address

【Configuration Example】1: Enable the abnormal alarm function.

```
AC-FS(config)# feedback user enable
```

【Verification】1: Use the show run command to view the configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

20.5mail-client check

Check that the email-related configuration takes effect

mail-client check

【Parameter Description】-

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】15

【Usage Guide】 After configuring the account and password of the smtp server and mailbox, use this command to check whether the configuration is successful. If the configuration is successful, the mailbox will receive a test email.

【Configuration Example】1: Check email configuration.

```
AC-FS# mail-client check
Connect to smtp server. OK!
Login to smtp server. OK!
Send a test mail. OK!
Check OK!
```

【Verification】Use a browser to log in to the mailbox to check whether the test email is received.

【Prompt Information】 1: The verification is successful.

```
Connect to smtp server. OK!
Login to smtp server. OK!
Send a test mail. OK!
Check OK!
```

2: No SMTP server or account is configured.

```
Check failed!
```

3: The smtp server is misconfigured, or dns is not configured.

```
Connect to smtp server. Failed!
```

4: Username or password is incorrect.

```
Send a test mail. Failed!
```

【Common Mistake】 1. smtp server configuration error.

2. Incorrect email account or password.

【Platform Description】 -

20.6mail-client smtp server

Check that the email-related configuration takes effect.

mail-client smtp server addr [port value]

Delete configuration.

no mail-client smtp server

【Parameter Description】

Parameter	Description
addr	smtp server address.
value	smtp server port number, value range: 1-65535.

【Default Configuration】-

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】It must be configured to send abnormal alarm emails.

The smtp server address can be found from the corresponding website, such as: smtp.qq.com, smtp.126.com.

In addition, the smtp service of some mailboxes (such as QQ mailbox) is disabled by default. After logging in to the mailbox with a browser, find this item in the setting options and set it to open.

【Configuration Example】1: Set SMTP server

```
AC-FS(config)# mail-client server smtp.126.com
```

【Verification】Use a browser to log in to the mailbox to check whether the test email is received.

【Prompt Information】-

【Common Mistake】 1. The smtp service is not enabled.

2. The smtp server address is wrong.

3. The device is not configured with dns.

【Platform Description】 -

20.7mail-client username

Configure email account password

mail-client username mail-addr password pw-string

delete configuration

no mail-client username mail-addr password pw-string

【Parameter Description】

Parameter	Description
username mail-addr	Email account number, generally in the format of xxx@yyy. The command does not check the format.
password pw-string	Email password.

【Default Configuration】-

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 Please confirm the following steps:

1: Use the email account applied for on the common email website. At present, 163, 126, 139, sina, qq, tom have been verified to be available. Other email accounts may also work, but have not been verified.

2: The mailbox supports smtp service. All the above email addresses are supported.

3: Use a browser to log in to the mailbox to see if the smtp service is enabled.

4: Log in to the email website and check the smtp server address.

【Configuration Example】1: Configure the account and password of the mailbox

```
AC-FS(config)# mail-client username AC-FS@qq.com password ******
```

【Verification】1: Use the show run command to check whether the configuration is successful.

【Prompt Information】 1: Delete failed. The email account was entered incorrectly or failed.

```
%error: please input right account_name(nabi@126.com) to delete!
```

2: Delete the email account successfully.

```
%notice: account_name(nabi@126.com) has been deleted
```

【Common Mistake】 1: The entered email account does not support smtp.

2: Mailbox is not enabled for smtp service.

3: The email account you entered has not been applied for through the website.

【Platform Description】 -

20.8mail-service enable

Enable mail service.

mail-service enable

close mail service.

no mail-service enable

【Parameter Description】-

【Default Configuration】 Enable

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 All functions related to sending emails need to open the email service.

【Configuration Example】1: Enable mail service.

```
AC-FS(config)# mail-service enable
```

【Verification】1: Use the show run command to check whether the configuration is successful.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

20.9mail-service source

Configure Mail Service Source IP.

mail-service source ip

Delete mail service source IP.

no mail-service source

【Parameter Description】

Parameter	Description
ip	Source IP address.

【Default Configuration】 None

【Command Mode】 Global mode

【Default Level】15

【Usage Guide】 It needs to be configured in public network mode, generally it is the IP of the internal network port.

【Configuration Example]】1: Configure the mail service source ip as 1.1.1.1.

```
AC-FS(config)# mail-service source 1.1.1.1
```

【Verification】1: Use the show run command to check whether the configuration is successful.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

20.10show feedback items

Check out the exception alert options.

show feedback items

【Parameter Description】-

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】15

【Usage Guide】 Use this command to view the alarm options supported by the device.

【Configuration Example]】1: View the currently supported alarm options.

```
AC-FS#show feedback items

no. name                    ignore -
4, CPU temperature too high,          NO
5,  Device under attack,              NO
6,  Total bandwidth exceeds the limit,    NO
7,  Flow control anomaly,             NO
8,  The main board temperature is too high,         NO
```

Field Description:

Field	Description
no.	Option ID.
name	Option description.
ignore	Is it configured to ignore.

【Prompt Information】 1: If the feedback template fails to load, there will be no display.

【Platform Description】 -

21 USER-TASK

21.1 clear user-task

Clear the user task log.

clear user-task

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】15

【Usage Guide】 This command is used to clear the task log of user tasks.

【Configuration Example]】1: Clear the user task log.

```
AC-FS# clear user-task
```

【Prompt Information】 None

【Platform Description】 -

21.2 show user-task

View user task information.

show user-task [log]

【Parameter Description】

Parameter	Description
log	View user task logs.

【Command Mode】 Privileged mode, global configuration mode

【Default Level】15

【Usage Guide】 Use this command to view the user task list and user task log.

【Configuration Example]】 1: View all user task lists.

```
AC-FS#sh user-task
User-task: enable
User-task log: enable
Time             Name             Mode Loop Command-sequence 2014-
09-22 15:00 remove static binding     config -- ip dhcp pool
my_pool
```

Field Description:

Field	Description
Time	task time.
Name	task name.
Mode	Command Mode.
Loop	Whether to cycle the task, cycle time.
Command-sequence	Sequence of CLI commands to execute.

2: View the user task log.

```
AC-FS# configure terminal AC-FS(config)#
user-task log enable AC-FS(config)# exit
AC-FS# show user-task log
```

【Prompt Information】

```
----------------------------

Task name: yyyy

Task time: 2014-09-19 16:09

Execute time: 2014-09-19 15:09

Execute mode: exec

Command: #wri

Result:  #

Building configuration...

  [OK]
```

```
_____

Task name:custom app

group

Task time: 2014-09-18 19:03

Execute time: 2014-09-19 15:14

Execute mode: config

Command: #identify-application custom-group test-group

Command: #app-add
```

【Platform Description】 -

21.3 user-task

Add user task

user-task add task-name command cli-string mode { exec | config } [date YYYY MM DD] time hh:mm

[every HH]

Delete user task.

user-task delete task-name

Modify User Tasks.

user-task modify task-name { mode { exec | config } | date YYYY MM DD | time hh:mm | every HH }

【Parameter Description】

Parameter	Description
task-name	The task name, which cannot exceed 16 bytes.
command cli-string	The CLI command sequence to be executed, the total length of the sequence cannot exceed 512 bytes. If there is a space in the command, use double quotes before and after the command, including the "@" symbol between subcommands Supports command abbreviations, e.g. "sh ip int br"
mode { exec | config }	Command Mode, exec is the privileged mode, and config is the global configuration mode.
date YYYY MM DD	The year, month, and day of the task execution. If no date is specified, it defaults to the current day. If the task date is not configured and the task time is earlier than the current time, the task date defaults to the next day
time hh:mm	Task execution time, from 00:00 to 23:59. Note: If the configured date+time is less than the current date+time, the configured commands will be executed immediately, including the reload command!
every HH	Task cycle time, supports 1-168 hours (ie 1 hour-1 week). When the task cycle time is configured, the task will be executed repeatedly according to the cycle time. If not configured, it will not cycle.

【Command Mode】 Privileged mode

【Default Level】15

【Usage Guide】 This command is used to add, delete and modify user tasks. After successful addition, the tasks will exist in the task library, and the system will execute the configured tasks regularly according to the task execution time. To delete and modify tasks, you need to specify the task name. When modifying a task, if you need to modify multiple properties, you must modify the configuration multiple times, one property at a time.

【Configuration Example]】1: Add a user task to reboot the device at 4:30 PM on September 2, 2014.

```
AC-FS# user-task add reload-task command "reload@y" mode exec date 2014 9 2 time 16:30
```

2: Delete a task named test.

```
AC-FS# user-task delete test
```

2: Modify an acyclic task named aa to be executed at 12 noon every day.

```
AC-FS# user-task modify aa every 24

AC-FS# user-task modify aa time 12:00
```

【Prompt Information】 1: If the input task name is too long, the configuration fails

```
USER-TASK: Task name len 22 is more than 16 bytes!
```

2: If the input command is too long, the configuration fails

```
USER-TASK: Command len 567 is more than 512 bytes!
```

3: If the entered task name already exists, adding the task fails

```
USER-TASK: Task name exists!
```

4: If the entered task name does not exist, the deletion/modification of the task fails.

```
USER-TASK: No such task named test!
```

5: When modifying the task time/date, if the total time and date entered is less than the current time and date, the modification will fail.

```
USER-TASK: New time is less than current time!
```

6: If the database is abnormal, the configuration will fail.

```
USER-TASK: Unexpected database error!
```

7: If the number of tasks exceeds 1000, the new task will fail.

```
USER-TASK: Too more tasks!(Not support more than %d tasks)
```

【Common Mistake】 1: The command Parameter is not quoted, resulting in configuration failure.

【Platform Description】 -

21.4 user-task enable

Start user task function

user-task enable

Turn off user tasks

no user-task enable

【Parameter Description】-

【Default Configuration】 Enable user task function

【Command Mode】 Global configuration mode

【Default Level】15

【Usage Guide】If the device is restarted or the user task is closed and other reasons cause the task not to be executed in time, and there are tasks with a task time earlier than the current time in the task library, the first task execution after the function is enabled will execute all the timed out tasks. Once again, if it is a recurring task, the next task time is calculated according to the task planning time and the recurring interval.

【Configuration Example】1: Enable user task function

```
AC-FS(config)# user-task enable
```

【Verification】1: Use the show user-task command to check whether the user task is enabled or disabled.

2: Use the show run command to check whether the user task is enabled or disabled.

【Prompt Information】 None

【Common Mistake】-

【Platform Description】 -

21.5 user-task log

Start the user task log function

user-task log enable

Disable the user task log function

no user-task log enable

【Parameter Description】-

【Default Configuration】 Disable task log function.

【Command Mode】 Global configuration mode

【Default Level】15

【Usage Guide】If the task to be configured and executed includes the show command, etc. and needs to pay attention to the task execution result, the task log function must be enabled to record the task execution result.

The device keeps logs for up to 30 days.

Device logs can be saved up to 20MB.

【Configuration Example]】1: Enable the user task log function

```
AC-FS(config)# user-task log enable
```

【Verification】1: Use the show user-task command to check whether the user task is enabled or disabled.

2: Use the show run command to check whether the user task is enabled or disabled.

【Prompt Information】 None

【Common Mistake】-

【Platform Description】 -

Chapter 11 Behavior Management

This volume introduces content related to behavior management and includes the following chapters:

1. layer23
2. APP-IDENTIFY
3. Global session limit
4. FLOW-CONTROL
5. FLOW-AUDIT
6. CONTENT-AUDIT

1 layer23

1.1 layer23 classify enable

Enable the second and third layer classification recognition function.

layer23 classify enable

Disable the classification and recognition function of the second and third layers.

no layer23 classify enable

【Parameter Description】-

【Default Configuration】 By default, the classification and recognition function of the second and third layers is enabled.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】After enabling Layer 2 and Layer 3 classification recognition, it supports vid-based, source ip or source mac, and destination ip-based object recognition.

【Configuration Example]】1: Enable the second and third layer classification recognition.

```
AC-FS(config)# layer23 classify enable
```

2: Turn off the second and third layer advertising mode.

```
AC-FS(config)# no layer23 classify enable
```

【Verification】1: Use the show run | in layer23 command to check whether the layer23 classify enable is displayed, and you can check whether the current configuration enables the layer23 classification recognition function.

2: Use the show layer23 obj-info command to check whether the second or third layer classification and identification function is enabled in the kernel.

【Prompt Information】-

【Common Mistake】 Layer 2 and 3 classification and identification are not enabled, resulting in user-based flow control, auditing and

other policies cannot take effect.

【Platform Description】

1.2layer23 deny-mode enable

Enable layer 2 and layer 3 global shielding mode.

layer23 deny-mode enable

Disable Layer 2 and Layer 3 global shielding mode.

no layer23 deny-mode enable

【Parameter Description】-

【Default Configuration】 By default, the global shielding mode of Layer 2 and Layer 3 is disabled.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】After the Layer 2 and 3 global shielding mode is enabled, all packets are discarded by default unless the user object is added to the whitelist (that is, excluding shielded users).

【Configuration Example】1: Enable global shielding mode.

```
AC-FS(config)# layer23 deny-mode enable
```

2: Turn off the global shield mode.

```
AC-FS(config)# no layer23 deny-mode enable
```

【Verification】1: Use the show layer23 deny-mode command to check whether the Layer 2 and Layer 3 shielding mode is enabled or disabled.

2: Use the show run | in layer23 command to check whether the layer23 deny-mode enable is displayed, and you can check whether the current configuration enables the global shielding mode of the second and third layers.

3: Use the show layer23 obj-info command to check whether the global shield mode is enabled in the kernel.

【Prompt Information】-

【Common Mistake】-

【Platform Description】

1.3layer23 flow-detect

Enable Layer 2 and Layer 3 traffic monitoring/configure traffic monitoring traffic and time interval.

layer23 flow-detect { enable | flow flowrate | time-interval time }

Disable the offline function of Layer 2 and Layer 3 traffic detection.

no layer23 flow-detect { enable | flow flowrate | time-interval time }

【Parameter Description】

Parameter	Description
enable	Flow detection offline switch.
flow flowrate	Configure traffic.
time-interval time	Configuration time interval.

【Default Configuration】 By default, the offline detection of Layer 2 and Layer 3 traffic is disabled.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】After enabling the Layer 2 and 3 traffic detection function, authenticate the online IP and account through the device. When the traffic within a specific time interval cannot reach the configured traffic Parameter, the device will actively kick the IP node offline. If there is a linkage with a third party, the third party will be notified to go offline.

【Configuration Example]】1: Enable the traffic detection function, and configure the offline without traffic for 30 minutes.

```
AC-FS(config)# layer23 flow-detect enable AC-
FS(config)# layer23 flow-detect flow 0
AC-FS(config)# layer23 flow-detect time-interval 30
```

2: Turn off the flow detection function.

```
AC-FS(config)# no layer23 flow-detect
```

【Verification】1: Use the show layer23 flow-detect command to check whether the flow detection function is enabled and configure Parameter.

2: After using the built-in local authentication to go online, enable the Layer 2 and 3 traffic detection function, configure the 15-minute no-traffic detection and go offline, change the IP address of the PC, and wait for 15 minutes before the IP is actively kicked off the line by the device.

【Prompt Information】-

【Common Mistake】-

【Platform Description】

1.4layer23 sam-accip-relate enable

Enable sam account association group name function.

layer23 sam-accip-relate enable

Disable the sam account association group name function.

no layer23 sam-accip-relate enable

【Parameter Description】-

【Default Configuration】 By default, this function is disabled.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 After enabling this function, the second and third layers will recognize the real-name information that will be synchronized with the sam server, including ip, account, and group. Since the unique name on the device side cannot belong to multiple parent groups, the account name is combined in the form of group name:name:account on the device side to ensure the uniqueness of the name. This function is only valid for users synchronized by the sam server.

【Configuration Example]】1: Enable the sam account associated group name function.

```
AC-FS(config)# layer23 sam-accip-relate enable
```

2: Disable the sam account associated group name function.

AC-FS(config)# no layer23 sam-accip-relate enable

【Verification】 1: Use the show layer23 sam-acc command to check whether this function is enabled or disabled.

2: 2: Use the show run | in layer23 command to check whether the layer23 scc-attention enable is displayed, and you can check whether the real-name information setting scc function is enabled in the current configuration.

3: After the sam account is synchronized to the device, show auth-subs brief to check whether the name is combined with the group name.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

1.5layer23 scc-attention enable

Enable the real-name information setting scc function.

layer23 scc-attention enable

Disable the real-name information setting scc function.

no layer23 scc-attention enable

【Parameter Description】 -

【Default Configuration】 By default, this function is enabled.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 After enabling this function, set the received server real-name information to the scc entry, and then set it to the aclk entry for releasing users. Note: In general, this option can be turned off to optimize device processing performance.

When authentication is enabled on both the switch and the device, this function must be enabled if authentication is not required on the device after the access switch is authenticated. In this scenario, some access switches do not have the authentication function, and some have the authentication function. The customer hopes that users who have passed the authentication on the access switch do not need to

be authenticated twice, and users who are not considered to be authenticated on the device side.

【Configuration Example]】1: Enable the real-name information setting scc function.

```
AC-FS(config)# layer23 scc-attention enable
```

2: Turn off the real-name information setting scc.

```
AC-FS(config)# no layer23 scc-attention enable
```

【Verification】1: Use the show layer23 state command to check whether the function is enabled or disabled.

2: Use the show run | in layer23 command to check whether the layer23 scc-attention enable is displayed, and you can check whether the real-name information setting scc function is enabled in the current configuration.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.6 network-group

Change the parent object path of the network object.

network-group str1 move to parent str2

【Parameter Description】

Parameter	Description
str1	Name of the network object to be moved.
str2	The name of the parent object after the move.

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 This command is mainly used to change the path to which it belongs without changing other properties under the original network object and the hierarchical structure of its child nodes.

【Configuration Example]】1: Move userA originally in the root directory to group1.

```
AC-FS# network-group userA move to parent group1
```

【Verification】Use the show network-group brief command to check whether the current network object organization hierarchy query is successfully moved.

【Prompt Information】 1: The name of the network object to be moved does not exist.

```
can not find the child-network.
```

2: The parent object name to which it belongs after the move does not exist.

```
can not find the parent-network.
```

3: You cannot move to your own name.

```
cann't move to parent of yourself.
```

4: The root object cannot be moved.

```
cann't move the root.
```

5: Move to its original parent object name, no need.

```
the network needn't to be moved.
```

6: Objects whose parent object is not a group cannot be moved.

```
childs of the range-network can not be moved.
```

7: The parent object after the move can only be a group object.

```
the parent after changed should be the network group!
```

8: Cannot move to its own child node.

```
cann't move to the child of yourself.
```

9: The depth of the tissue structure after the move exceeds the maximum limit.

```
the depth of the network moving is more than 5!
```

10: Objects created by the system by default cannot be moved.

```
can not move the system default group.
```

【Common Mistake】 1: The number of levels after the move exceeds the limit, resulting in failure to move successfully. 2: The system default object cannot be moved.

【Platform Description】 -

1.7 network-group export

Export the network object configuration in the current system to a file.

network-group export { txt | csv } filename

【Parameter Description】

Parameter	Description
filename	File Name.

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】This command is mainly used to export network objects in batches, and export the current network object configuration in the system to an external file.

【Configuration Example]】1: Export the network object configuration to the file "ip-info.txt".

```
AC-FS# network-groupexport txt ip-info.txt
```

【Verification】Use show network-groupall and show network-group brief to open ip-info.txt to check whether the current configuration has been imported into the file.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.8 network-group import

Import network objects into the current configuration.

network-group import { txt | csv } filename [overwrite]

【Parameter Description】

Parameter	Description
filename	File Name
overwrite	Conflict Mode Flag

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 This command is mainly used to batch import network objects to the current configuration macro.

The format of writing network objects in the txt format file is as follows: each line of the file represents a network object, and the order of each element of the object is: path, object name, ip address. Each element in the network object is separated by ",". Items with no content can be left blank, but "," should be reserved. For example, if the last column does not exist, then keep "," at the end of the line.

The following is an example of a network object record in a ".txt" network object file:

/all users/usergroup1,user1,192.168.197.1

The file in csv format can be obtained by editing it in Microsoft Excel and clicking save as ".csv". The editing format of the records in the file is: a record is divided into 4 columns, which are: parent object path, object name, and object ip address.

In normal mode, the creation of conflicting network objects fails. In overwrite mode, all conflicting network objects including name conflicts, ip conflicts will be deleted and new objects will be created.

【Configuration Example]】1: Import the network object file "ip-info.txt".

```
AC-FS# network-groupimport txt ip-info.txt
```

【 Verification 】 Use show network-groupall and show network-group brief to check whether the current configuration contains successfully imported network objects.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.9 network-group name

Configure the network object.

network-group name namestr [parent parent] [ip-host ip-addr | ip-subnet subnet mask | ip-range start end]]

Delete network objects.

no network-group name namestr

【Parameter Description】

Parameter	Description
namestr	Network Object Name.
parent	Path to which the parent object belongs.
ip-addr	Single IP object IP address.
subnet	IP segment start address.
mask	Mask.
start	IP range start address.
end	IP range end address.

【Default Configuration】 By default, the system creates the Out_Server network object by default.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】Network objects only have ip address information, which are divided into three types: single ip address network objects, ip address segment network objects, and ip address range network objects.

There is a default object "/" by default. When the second and third layer classification recognition is enabled, if the destination IP address of the packet does not match any other network object, the default object "/" is matched by default. When parent Field is not set, it defaults to the root directory.

Network object names are unique and cannot be the same between different network object names.

【Configuration Example]】1: Configure the ip address segment network object "network1", including the 192.168.196.0 network segment, its parent object is "user group 1", and the parent object of "user group 1" is "all user groups".

```
AC-FS(config)# network-group name network1parent /All user groups / user groups 1 ip-subnet 192.168.196.0
255. 255. 255. 0
```

【Verification】Use show network-groupall to view all information about network objects.

【Prompt Information】 1: The network object does not exist.

```
can not find this network!
```

2: Objects created by the system by default are not allowed to be deleted.

```
cannot delete the network default group.
```

3: The path to which the parent object belongs is wrong.

```
Parent string error.
```

4: The configured parent object is wrong.

```
parent subscriber error.
```

5: Name and xxx conflict.

```
name conflict with xxx.
```

6: Network object groups and network objects cannot be exchanged.

```
network group and network can not exchange
```

7: Conflict with xxx object ip configuration.

```
ip conflict with xxx.
```

8: The ip address is wrong.

```
ip address error.
```

9: The parent object of a range object can only be a user group.

```
parent of ip range network must be network group.
```

10: ip or mask error.

```
ip or mask error
```

【Common Mistake】-

【Platform Description】 -

1.10 network-group rename

Rename the network object name.

network-group rename oldname newname

【Parameter Description】

Parameter	Description
oldname	Original network object name.
newname	New network object name.

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 This command is mainly used to change the name of the network object without changing other properties of the original network object.

【Configuration Example]】1: Rename the network object named userA to userB.

```
AC-FS# network-grouprename userA userB
```

【Verification】 Use show network-group by-name userB to check whether the object and other properties have changed before renaming.

【Prompt Information】 1: The new name already exists.

```
name is conflict with other network.
```

2: The old name network object does not exist.

```
can not find this network
```

3: The system does not allow renaming of objects created by default.

can not rename the network default group.

【Common Mistake】-

【Platform Description】 -

1.11 show auth-subs

View the authentication object information.

show auth-subs [all | brief | parent [name | root]]

【Parameter Description】

Parameter	Description
all	Display account information of all authentication objects.
brief	Displays the authentication object account organization hierarchy.
parent	Displays the sub node information of the authentication object account.
name | root	Authentication object account name or root object.

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】 14

【Usage Guide】 It is used to display the configuration information of the authentication object, and different forms of network object information can be displayed by specifying keywords.

【Configuration Example]】1: View the details of all authentication object accounts.

```
name                                                    dir type index
smp_root                                                 1  2  2
sam_root                                                1 4 3
webauth_root                                            1    1   4
```

Field Description:

Field	Description
name	Authentication object name.
dir	Authentication object group.

type	Authentication object type (1-auth, 2-smp, 3-smp + auth4-sam).
index	Authentication object index value, uniqueness.

【Prompt Information】 -

【Platform Description】 -

1.12 show network-group

View network object information.

show network-group [all | brief | parent [name | root]]

【Parameter Description】

Parameter	Description
all	Display all network object information.
brief	Displays the network object organization hierarchy.
parent	Displays the information of the child nodes of the network object.
name | root	Network object name or root object.

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】 14

【Usage Guide】 It is used to display the configuration information of network objects, and different forms of network object information can be displayed by specifying keywords.

【Configuration Example]】 1: View the detailed information of all network objects.

```
name                            dir index ip
root                             1 1
Out_Server                       1  2
ii                               1   18093
jj                               1  14691
uu                               0   32105 6.6.6.3 - 6.6.6.5
uuii                             1   12652
```

Field Description:

Field	Description
name	Network object name.
dir	Network object group properties.
index	Network object index value, uniqueness.
ip	Configure network object IP address.

【Prompt Information】-

【Platform Description】 -

1.13show subscriber

View user object information.

show subscriber [all | brief | parent [name | root] | custom-group {all | name namestr relate-all}]

【Parameter Description】

Parameter	Description
all	Display all user object information.
brief	Displays the user object organization hierarchy.
parent	Displays the information of the child nodes of the user object.
name | root	User object name or root object.
custom-group	Displays all user-defined groups and their associated IP segment information.
all | name	Displays information associated with all custom groups or specific custom groups.
namestrrelate-all	Customize all information associated with the group object name.

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】 14

【Usage Guide】 It is used to display the configuration information of user objects, and different forms of user object information can be displayed by specifying keywords.

【Configuration Example]】1: View the detailed information of all user objects.

```
name                                mac                dir av-fc av-con vip rel deny pwd-e au-deny login
vpn vbr webauth ssl-deny bind h-pwd idx        ssl-radius ip
root                                0000.0000.0000   1    0     0      0   0   0    0     0
0     1   0   1   0    0    0     1          0
Default_Group                       0000.0000.0000   1    0     0      0   0   0    0     0
0     1   0   1   0    0    0     2          0
without_auth_user                   0000.0000.0000   0    0     0      0   0   0    0     0
0     0   0   1   0    0    1     4          0
xxy                                 0000.0000.0000   1    0     0      0   0   0    0     0
0     1   0   1   0    0    0     549939033 0
tt                                  0000.0000.0000   0    0     0      1   0   0    0     0
0     1   0   1   0    2    0     3445540573 0.................3.3.3.6
Vpn_Group                           0000.0000.0000   1    0     0      0   0   0    0     0
0     1   0   1   0    0    0     3          0
five                              0000.0000.0000   1    0     0      0   0   0    0     0
0     1   0   1   0    0    0     912778062 0
ee                                  0000.0000.0000   0    0     0      0   1   0    0     0
0     1   0   1   0    2    0     680907908 0          192.168.3.81
xhl                                 0000.0000.0000   0    0     0      0   0   0    0     0
0     1   0   1   0    2    0     310883589 0          172.18.3.81
eg                                  0000.0000.0000   0    0     0      0   0   0    0     0
0     1   0   1   0    2    0     2753766751 0          172.18.3.100 - 172.18.3.250
uiiu                                3333.3333.3333   0    0     0      0   0   0    0     0
0     1   0   1   0    1    1     2364943795 0
ttt                                 0000.0000.0000   1    0     0      0   0   0    0     0
0     1   0   1   0    0    0     1938928104 0
```

Field Description:

Field	Description
name	User object name.
mac	Configured MAC address.
dir	User object group properties.
av-fc	Flow control free sign.
av-con	Identification and audit free marks.
vip	vip logo.
rel	Whitelist attribute flag.
deny	Mask attribute flag.

pwd-e	Modify password attribute flag.
au-deny	Disable web authentication login attribute flag.
login	Login authentication permissions.
vpn	vpn authentication permissions.
vbr	vpn branch logo.
webauth	web authentication permissions.
ssl-deny	Disable sslvpn authentication login attribute.
bind	Binding flag: 0 - no binding, 1 - one-way binding, 2 - two-way binding.
h-pwd	Contains a password symbol.
idx	Object index value.
ssl-radius	sslvpn account server-side checksum attributes.
ip	Configured ip address.

2: View details of all custom groups.

```
AC-FS#show subscriber custom-group all
name                                custom  cnt    index
XIA                              1        1     2973161921
yanjiuyuan                         1       2     3332760464
555  1  1  1040419816
556                                1       1     754996415 ttt
```

Field Description:

Field	Description
name	User object name.
custom	1 indicates a custom group, 0 indicates a non-custom group.
cnt	Number of nodes associated with this custom group.
index	Indexes corresponding to custom groups.

3: View the details of the associated node of the custom group yanjiuyuan.

```
AC-FS#show subscriber custom-group name yanjiuyuan relate-all
yanjiuyuan relate-all:
    172.18.124.10 - 172.18.124.10
    172.18.124.1 - 172.18.124.255
```

【Prompt Information】-

【Platform Description】 -

1.14 show vlan-group

View vlan object information.

show vlan-group [name-str]

【Parameter Description】

Parameter	Description
name-str	Displays information about the specified VLAN object.

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】 14

【Usage Guide】 Used to display vlan object information.

【Configuration Example]】1: View the detailed information of all vlan objects.

Parameter	Description
name-str	Displays information about the specified VLAN object.

Field Description:

Field	Description
name	VLAN object name.
index	VLAN object index value.
vlan_id	The vid contained in the vlan object.

【Prompt Information】-

【Platform Description】 -

1.15subscriber

Move the user object under another object.

subscriber str1 move to parent str2

【Parameter Description】

Parameter	Description
str1	Name of user object to be moved.
str2	The name of the parent object after the move.

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 This command is mainly used to change the path to which it belongs without changing other attributes under the original user object and the hierarchical structure of its child nodes.

【Configuration Example]】1: Move userA originally in the root directory to group1.

```
AC-FS#subscriber userA move to parent group1
```

【Verification】Use the showsubscriber brief command to check whether the current user object organization hierarchy query is successfully moved.

【Prompt Information】 1: The name of the user object to be moved does not exist.

```
can not find the child-subs.
```

2: The parent object name to which it belongs after the move does not exist.

```
can not find the parent-subs.
```

3: You cannot move to your own name.

```
cann't move to parent of yourself.
```

4: The root object cannot be moved.

```
cann't move the root.
```

5: Move to its original parent object name, no need.

```
the subscriber needn't to be moved.
```

6: Objects whose parent object is not a group cannot be moved.

```
childs of the range-subscriber can not be moved.
```

7: The parent object after the move can only be a group object.

```
the parent after changed should be the subscriber group!
```

8: Cannot move to its own child node.

```
cann't move to the child of yourself.
```

9: The depth of the tissue structure after the move exceeds the maximum limit.

```
the depth of the subscriber moving is more than 5!
```

10: Objects created by the system by default cannot be moved.

```
can not move the system default subs.
```

【Common Mistake】 1: The number of levels after the move exceeds the limit, resulting in failure to move successfully. 2: The system default object cannot be moved.

【Platform Description】 -

1.16subscriber allow

Set the permission to use the user object account.

subscriber allow string privilege { none | { [webauth] [vpn] [login] } }

The no command permission setting does not take effect, and the newly configured permission command will overwrite the original permission configuration.

【Parameter Description】

Parameter	Description
string	User object account name.
none	No permissions are allowed.
webauth	web authentication permissions.
vpn	vpn authentication permissions.
login	login authentication permissions.

【Default Configuration】 By default, the vpn authentication authority and web authentication authority of the user object account are allowed.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 To set the usage authority of the account, you can not allow or allow login authentication, one of vpn authentication and web authentication, the second, and the third.

The login authentication currently does not support using the account authentication of the user management office.

【Configuration Example]】 1: Set "User 1" vpn permission and login permission.

```
AC-FS(config)#subscriber allow user 1 privilegevpn login
```

2: Set "User 1" all permissions are not allowed.

```
AC-FS(config)# subscriber allow user 1 privilegenone
```

【Verification】 Use show subscriber by-namestr to check whether the login, vpn and webauth flags under a user object are 1, indicating whether the corresponding permission is enabled.

【Prompt Information】 1: The user object does not exist.

```
name                                mac               dir av-fc av-con vip rel deny pwd-e au-deny login
vpn vbr webauth bind h-pwd idx      ip
xhl                                 0000.0000.0000    0     0      0       0   0   0     0      0        0
1   0   1       2    0     310883589 172.18.3.81
```

2: The system default object account is not allowed to set permissions.

```
can not set privi to the system default subs.
```

3: The user object group is not allowed to set permissions.

```
can not set privi to subscriber group.
```

【Common Mistake】 1: The number of levels after the move exceeds the limit, resulting in failure to move successfully. 2: The system default object cannot be moved.

【Platform Description】 -

1.17subscriber export

Export the user object configuration in the current system to a file.

subscriber export { txt | csv } filename

【Parameter Description】

Parameter	Description
filename	filename

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 This command is mainly used to export user objects in batches, and export the current user object configuration in the system to an external file.

【Configuration Example]】1: Export the user object configuration to the file "user-info.txt".

```
AC-FS#subscriber export txt user-info.txt
```

【Verification】Use show subscriber all and show subscriber brief to open user-info.txt to check whether the current configuration has been imported into the file.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.18subscriber import

Import the user object into the current configuration.

subscriber import { txt | csv } filename [overwrite]

【Parameter Description】

Parameter	Description
filename	filename
overwrite	Conflict Mode Flag

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 This command is mainly used to batch import user objects to the current configuration macro.

The format of the user object written in the txt format file is as follows: each line of the file represents a user object, and the order of each element of the object is: path, account name, password, ip address, MAC address, whether the two-way binding flag. Each element in the user object is separated by ",". Items without content can be left blank, but "," should be retained. For example, if the last column does not exist, then keep "," at the end of the line.

The following is an example of a user object record in a ".txt" user object file:

/all users/usergroup1,user1,,192.168.197.1,,

The file in csv format can be obtained by editing it in Microsoft Excel and clicking save as ".csv". The editing format of the records in the file is: a record is divided into 6 columns, which are: parent object path, object name, password, object ip address, mac, whether the two-way binding flag address.

In normal mode, conflict user creation fails. In overwrite mode, all conflicting user objects will be deleted including user name conflict, ip conflict, mac conflict then create new object.

【Configuration Example]】1: Import the user object file "user-info.txt".

```
AC-FS#subscriber import txt user-info.txt
```

【Verification】 Use show subscriber all and show subscriber brief to check whether the current configuration contains successfully imported user objects.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

1.19subscriber rename

Rename the user object name.

subscriber rename oldname newname

【Parameter Description】

Parameter	Description
oldname	Original user object name.
newname	New user object name.

【Default Configuration】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 This command is mainly used to change the name of the user object without changing other attributes of the original user object.

【Configuration Example]】1: Rename the user object named userA to userB.

```
AC-FS#subscriber rename userA userB
```

【Verification】Use show subscriber by-name userB to check whether the object and other properties have changed before renaming.

【Prompt Information】 1: The new name already exists.

```
name is conflict with other subscribers.
```

2: User object with old name does not exist.

```
can not find this subscriber
```

3: The system does not allow renaming of objects created by default.

```
can not rename the system default subs.
```

【Common Mistake】-

【Platform Description】 -

1.20subscriber set

Set user object special properties.

subscriber set namestr attribute {avoid-monitor[flow-monitor] | deny | release | vip | auth-deny |

pwd-edit | ssl-auth-deny | ssl-radius-verify}

Cancel the user for special attributes.

no subscriber set namestr attribute {avoid-monitor | deny | release | vip | auth-deny |pwd-edit | ssl-auth-deny | ssl-radius-verify }

【Parameter Description】

Parameter	Description
namestr	User object name.
avoid-monitor	No monitoring properties include no application identification, content audit, and traffic control.
flow-monitor	No monitoring and no flow control.
deny	Shield property.
release	White list properties. That is, to exclude the blocking user properties.
vip	vip attribute.
auth-deny	Login properties are prohibited.
pwd-edit	Allows you to modify the password properties.
ssl-auth-deny	Proable sslvpn authentication properties (based on group configuration).
ssl-radius-verify	sslvpn The local account password does not verify the attribute.

【Default Configuration】 By default, it does not contain any special properties.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 After setting the monitoring-free attribute, the user will not perform flow control, content auditing and application identification by default, but you can set flow-monitor to enable flow control for this user.

The masking attribute does not take effect in the masking mode. If the masking attribute is set in the normal mode, the packets of the user are discarded.

The shielding attribute takes effect only in the non-shielding mode. In the non-shielding mode, if the monitoring-free and shielding attributes are set at the same time, the shielding attribute takes precedence.

The whitelist attribute only takes effect in the shield mode. After the Internet shield mode is enabled, all users cannot access the Internet by default unless the user's whitelist attribute "release" is set.

The vip attribute is used to perform unified flow control processing on users. Static user objects with vip attribute set can be used for unified flow control processing.

The auth-deny attribute is used to set the authentication mask attribute of the account, which is only valid when the built-in authentication is enabled. After setting, users who are online with this account cannot be authenticated, and users who are online with this account will also be offline.

The pwd-edit attribute use case sets the authentication and modification password attribute of the account, which is only valid when the built-in authentication is enabled. After setting, users who go online with this account can change the password by themselves.

The ssl-auth-deny attribute is used to set the disabled sslvpn authentication attribute of the account (group). After setting, the account or accounts under this account group will not be able to pass sslvpn authentication.

The ssl-radius-verify attribute is used to set the sslvpn local account password of the account (group) without verifying the authentication attribute. After setting, the local account of sslvpn will not verify the password even if it exists, and the return timeout is convenient for the account and password verification on the radius server.

【Configuration Example]】1: Set "User 1" to be free of content auditing and application identification, but subject to traffic control.

```
AC-FS(config)#subscriber set user 1 attribute avoid-monitor flow-monitor
```

2: Remove the monitoring-free attribute of the user object "User 1".

```
AC-FS(config)#no subscriber set user 1attribute avoid-monitor
```

【Verification】Use show subscriber by-name userB to view all the information under the object.

【Prompt Information】 1: The user object does not exist.

```
can not find this subscriber.
```

2: The object created by the system by default does not allow special attributes to be set.

```
can not set attri to the system default subs.
```

3: The user object group does not support setting special attributes.

```
can not set attribute to subscriber group.
```

【Common Mistake】-

【Platform Description】 -

1.21 subscriber static

Configure a user object.

subscriber staticname namestr parent parstr [[[[ip-host ip-addr] [mac mac-addr] | ip-subnet subnetmask

| ip-range start end] [password pwd_str { two-way-bind | single-way-bind }]] | [password pwd_str]]

Delete a user object.

no subscriber static name namestr

【Parameter Description】

Parameter	Description
namestr	User object name.
parstr	Parent object path.
ip-addr	ip address.
mac-addr	mac address.
subnet	ip segment base.
mask	mask off code.
start	The ip range starting address.
end	ip range end address.
pwd_str	password.
two-way-bind	Two-way binding flag.
single-way-bind	One-way binding flag.

【Default Configuration】 By default, Vpn_Group, Default_Group and without_auth_user are created by default.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 The ip address of the user object cannot conflict with the user object other than the parent object, and the mac address cannot conflict with any other user object.

User objects are classified by ip address into three types: single ip address user object, ip address segment user object and ip address range user object. By mac address, there are two types of user objects that contain mac addresses and user objects that do not contain mac addresses. A user object with a single ip address can contain a mac address at the same time, but an ip address segment and an ip address range user object cannot contain a mac address at the same time. When the mac address and ip address are matched at the same time, the matching result of the mac address shall prevail.

There is a default user object "/" by default. When the Layer 2 and 3 classification recognition function is enabled, if the source IP address of the packet does not match any other user object, the default object is matched by default.

Ordinary user objects can be used as accounts after setting passwords. One-way and two-way binding is only for accounts with ip or mac. When two-way binding, the account and ip or mac are two-way bound, and the account can only use a certain IP or mac. The ip or mac can only be used by the account. In one-way binding, the account can only use the bound ip or mac, but this ip or mac address may also be used by other accounts.

An account that is not bound to ip and mac means that the account is not restricted by the ip or mac address used. Accounts with ip and mac are bound in both directions by default. Under the built-in authentication, after using the account to go online, it will be automatically added under the account, whether it is using the ip of the account in the tree to go online or add it under the webauth_root.

User object names are unique, and the names cannot be the same between different user objects.

【Configuration Example]】 1: Configure "User 1", the IP address is "192.168.196.156", its parent object is "User Group 1", and the parent object of "User Group 1" is "All User Groups".

```
AC-FS(config)# subscriber static name user 1 parent / all user groups / user group 1 ip-host 192.168.196.156
```

【Verification】 Use show subscriberall to view all user object information.

【Prompt Information】 1: The user object does not exist.

```
can not find this subscriber!
```

2: Objects created by the system by default are not allowed to be deleted.

```
cannot delete the default group.
```

3: The path to which the parent object belongs is wrong.

```
Parent string error.
```

4: The configured parent object is wrong.

```
parent subscriber error.
```

5: Objects with passwords cannot be used as parent objects.

```
parent subscriber cannot be the have-pwd-subs.
```

6: The parent object of an object with a password can only be a user group.

```
par of the have-pwd-subs must be the group.
```

7: Name and xxx conflict.

```
name conflict with xxx.
```

8: User groups and user objects cannot be exchanged.

```
subscriber group and subscriber can not exchange
```

9: A non-group object with child nodes cannot set a password.

```
the no-group subs had child-subs cannot set password.
```

10: Conflict with xxx object ip configuration.

```
ip conflict with xxx.
```

11: Conflict with xxx object ip configuration of one-way binding ip.

```
ip conflict with bind-single-way xxx.
```

12: Conflict with xxx object mac configuration.

```
mac conflict with xxx.
```

13: Conflict with the mac configuration of the xxx object that is one-way bound to the mac.

```
mac conflict with single-bind xxx.
```

14: The ip address is wrong.

```
ip address error.
```

15: The parent object of a range object can only be a user group.

```
parent of ip range subscriber must be subscriber group.
```

16: ip or mask error.

```
ip or mask error
```

17: The configured range object and the one-way binding IP xxx object ip configuration conflicts.

```
IP-RANGE: ip conflict with bind-single-way xxx.
```

【Common Mistake】 1: Misunderstanding of the concept of one-way and two-way binding.

2: The account permission configuration problem causes the authentication to fail.

【Platform Description】 -

1.22vlan-group

Configure the vlan object.

vlan-group name vlan vid-list

delete vlan object.

no vlan-group name

【Parameter Description】

Parameter	Description
name	vlan object name.
vid-list	object vid.

【Default Configuration】-

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】The vlan ids between vlan objects cannot conflict. Multiple vlan ids are separated by commas. If you need to configure multiple consecutive vlan ids to belong to the same vlan object, you can use "-" to separate the start vlan id and the end vlan id Indicates multiple consecutive vlan ids.

There is a default vlan object "any" by default. When the second and third layer classification recognition function is enabled, the default object "any" in all data flows in gateway mode is matched by default.

In bridge mode, all data streams match the vlan object corresponding to the bridge's native vlan by default. If the bridge's native vlan does not have a corresponding vlan object, the default object "any" in the data stream matching.

The names of different vlan objects cannot be the same, and the identification of vlan objects in gateway mode is invalid.

【Configuration Example]】1: Configure the vlan object "vlan-group1" to include vlan 1, vlan 3, vlan7, vlan8, and vlan9.

```
AC-FS(config)# vlan-group vlan-group1 vlan 1,3,7-9
```

【Verification】Use show vlan-groupall to view all information about vlan objects.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

2 APP-IDENTIYF

2.1app-add

Add an application to the user-defined application group.

app-add app-name

Deleting an app in a user-defined group.

app-del app-name

【Parameter Description】

Parameter	Description
app-name	Application name.

【Default Configuration】 By default, the new custom application group has no application.

【Command Mode】 custom-group Configure Command Mode

【Default Level】 14

【Usage Guide】 Use this command to add applications to the user-defined application group. The applications in the user-defined application group may be applications supported by the system, or may be application groups supported by the system.

【Configuration Example]】1: Add a journey game to the MYGAME custom application group.

```
AC-FS#config
AC-FS(config)#identify-application custom-group MYGAME
AC-FS(config-custom-group)#app-add  journey
```

【Prompt Information】 1: If the application does not exist, it will prompt:

```
AC-FS#config
AC-FS(config)#identify-application custom-g AC-FS(config)#identify-application custom-group aaa AC-FS(config-custom-
group)#app-add no_exit
This application is not exist!
```

2: Insufficient memory, then prompt:

```
AC-FS#config
AC-FS(config)#identify-application custom-g AC-FS(config)#identify-application custom-group Instant messaging software
not enouth memory!
```

3: If a custom application group is added to another custom application group, it will prompt:

```
AC-FS#config
AC-FS(config)#identify-application custom-group aaa
AC-FS(config-custom-group)#exit
AC-FS(config)#identify-application custom-group bbb
AC-FS(config-custom-group)#app-add aaa
One custom-group cannot join another custom-group!
```

【Common Mistake】 1: The application does not exist.

2: Custom app group joins another custom app group.

【Platform Description】 Wireless AC series products.

2.2app-del

Delete an app in a user-defined app group.

app-del app-name

Restore configuration.

app-add app-name

【Parameter Description】-

【Default Configuration】 By default, the new custom application group has no application.

【Command Mode】 custom-group Configure Command Mode

【Default Level】 14

【Usage Guide】 With this command, you can delete applications from the user-defined application group. The applications in the user-defined application group may be applications supported by the system, or may be application groups supported by the system.

【Configuration Example]】1: Delete the journey game from the MYGAME custom application group.

```
AC-FS#config
AC-FS(config)#identify-application custom-group MYGAME
AC-FS(config-custom-group)#app-del journey
```

【Prompt Information】 1: If the application does not exist, it will prompt:

```
AC-FS#config
AC-FS(config)#identify-application custom-group aaa
 AC-FS(config-custom-group)#app-del bcd
This application doesn't exist!
```

2: If the application is not added to the application group, it will prompt:

```
AC-FS#config
AC-FS(config)#identify-application custom-group aaa
 AC-FS(config-custom-group)#app-del Time communication software
The application doesn't join the custom-group!
```

【Common Mistake】 1: The application does not exist.

2: The app does not exist in the custom app group.

【Platform Description】 Wireless AC series products.

2.3 identify-application app-db enable

Turn on the app collection feature.

identify-application app-db enable

Turn off app collection.

no identify-application app-db enable

【Parameter Description】-

【Default Configuration】 Open by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】This command enables the application collection function.

【Configuration Example]】1: Enable the application collection function.

```
AC-FS#config
AC-FS(config)#identify-application app-db enable
```

【Common Mistake】-

【Platform Description】 Wireless AC series products.

2.4 identify-application block

Add an app to the blocking apps group.

identify-application block app-name

Move an app out of the blocking apps group.

no identify-application block app-name

【Parameter Description】

Parameter	Description
app-name	Application name.

【Default Configuration】Do not join the blocking application group by default

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to add an application to the blocking application group.

【Configuration Example]】1: Add the MSN application to the blocking application group.

```
AC-FS#config
AC-FS(config)#identify-application block MSN
```

【Verification】1: Use the show identify-application block command to view all applications in the blocked application group.

【Prompt Information】 1: If an application is already in other system application groups, it will prompt an error. If MSN has been added to the blocking group, and the MSN application is added to the blocking application group, it will prompt:

```
AC-FS(config)#identify-application block MSN
The application has already been joined Inhibitive_Group!
```

2: If an application that does not exist is added to the blocking application group, it will prompt that the application does not exist.

```
AC-FS(config)#identify-application block XXX
The application does not exist!
```

【Common Mistake】 1: An application has been added to other system application groups.

2: Application does not exist.

【Platform Description】 Wireless AC series products.

2.5 identify-application custom-group

Added user-defined application groups.

identify-application custom-group group-name

Delete user-defined application groups.

no identify-application custom-group group-name

【Parameter Description】

Parameter	Description
group-name	application group name.

【Default Configuration】 By default, there is no user-defined application group

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command can be used to add user-defined application groups.

Users can define up to 100 types of user-defined application groups.

After this command is configured, the command configuration mode transfers to the custom-group configuration command layer.

【Configuration Example]】1: The following command adds a user-defined MYGAME application group: the level of the application group is the same as the key application group, and the suppression application group is the same.

```
AC-FS#config
AC-FS(config)#identify-application custom-group MYGAME
AC-FS(config-custom-group)#
```

【Prompt Information】 1: Delete a custom application group that does not exist, then prompt:

```
AC-FS(config)#no identify-application custom-group abc
The custom-group doesn't exist!
```

2: If the name of the custom application group conflicts with the application in the system, it will prompt:

```
AC-FS(config)#id custom-group Instant messaging software
The application name is conflict with application in system!
```

3: If the number of application groups exceeds the maximum value, it will prompt:

```
AC-FS(config)#id custom-group group101
The number of custom-group cannot be more than 100!
```

【Common Mistake】 1: The name of the custom application group conflicts with the application in the system 2: The number of custom application groups exceeds the upper limit.

【Platform Description】 Wireless AC series products

2.6 identify-application clear key-inhibitive-block-other group

Clear key application groups, suppress application groups and block all applications in application groups.

identify-application clear key-inhibitive-block-other group

【Parameter Description】-

【Default Configuration】-

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】An application can be added to the key application group, the inhibited application group, or the blocking application group, but it cannot be added to both the key application group and the inhibited application group at the same time. group, suppress application group and block application deletion in application group.

【Configuration Example]】1: Delete all applications from the key application group, the suppression application group and the blocking application group.

```
AC-FS#config
AC-FS(config)# identify-application clear key-inhibitive-block-other group
```

【Verification】1: Use the show identify-application key, show identify-application inhibitive, show identify-application-block and show identify-application other commands to view all applications in the key, inhibit, block and other application groups.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 Wireless AC series products.

2.7 identify-application custom name

Configure a user-defined rule.

identity-application custom name software-name class class-name { ip sip { any any | sip-low sip-high } dip { any any | dip-low dip-high } | { tcp | udp } { sport { any any | sport-low sport-high } dport { any any | dport-low dport-high } | { sip { any any | sip-low sip-high } { sport { any any | sport-low sport-high } | dip
{ any any | dip-low dip-high } } | dip { any any | dip-low dip-high } dport { any any | dport-low dport-high } } } }

Move an app out of the blocking apps group.

no identity-application custom name software-name class class-name { ip sip { any any | sip-low sip-high } dip { any any | dip-low dip-high } | { tcp | udp } { sport { any any | sport-low sport-high } dport
{ any any | dport-low dport-high } | { sip { any any | sip-low sip-high } { sport { any any | sport-low sport-high } | dip { any any | dip-low dip-high } } | dip { any any | dip-low dip-high } dport { any any | dport-low dport-high } } } }

【Parameter Description】

Parameter	Description
software-name	Application software name.
class-name	Application category name.
sport-low	Start source port.Range 0-65535 or any.
sport-high	End the source port.Range 0-65535 or any.
dport-low	Start with the destination port.Range 0-65535 or any.
dport-high	End of the destination port.Range 0-65535 or any.
sip-low	Start source ip (ipv4 or ipv6, the same below).
sip-high	End source ip.
dip-low	Starting destination ip.
dip-high	End of the purpose ip.

【Default Configuration】 No user-defined rules by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 You can add a user-defined rule by configuring this command.

User-defined applications support the configuration of the following types of user-defined applications:

1. Protocol type, source port, destination port

2. Protocol type, source ip, source port

3. Protocol type, source ip, destination ip

4. Protocol type, destination ip, destination port

User-defined applications have the following restrictions on rules:

1. For the "protocol type, source port, destination port" type rule, the source port and destination port cannot be any at the same time.

2. For the "protocol type, source ip, source port" type rule, source ip and source port cannot be any

3. For the "protocol type, source ip, destination ip" type rule, the source ip and destination ip cannot be any at the same time

4. For the "protocol type, destination ip, destination port" type rule, neither destination ip nor destination port can be any

5. You can configure a single ip or an ip segment, but the range of the ip segment cannot exceed 32 ips, and the ip segment must be continuous.

6. Under the existing application category name and application name in the system, user-defined application features can be added. The existing system application classification features and system application features are not affected, but the priority is not as high as user-defined.

7. The user-defined application category name supports up to 31 characters, and the user-defined software name supports up to 27 characters. The user-defined application category name of AC products supports up to 63 characters, and the user-defined software name supports up to 59 characters.

8. Customize the application of the same source ip or destination ip, you can configure the number of discontinuous destination ports or source ports at most. Example: destination ip + destination port type, ip: 1.1.1.1 + port: 80, ip: 1.1.1.1 + port: 100 , ip:1.1.1.1 + port:200, so that only 16 ip+port pairs of the same ip can be configured at most

9. If the starting source ip is ipv4 (or ipv6), all remaining ips within the range covered by the command can only be ipv4 (or ipv6) 10. Neither the source ip nor the destination ip range can be specified as 0 (regardless of ipv4 or ipv6))

【Configuration Example]】 1: Configure a user-defined rule, the application is classified as a custom game, the application name is Xunlei Game, the source port range is 1 to 10, the destination port range is 1 to 100, and the protocol type is tcp:

```
AC-FS#config
AC-FS(config)#identify-application custom name Thunder Games class  custom game  tcp sport 1 10 dport 1
```

2: Configure a user-defined rule, the application classification is myp2p, the application name is myxunlei, the source port is arbitrary, the destination port range is 200, and the protocol type is udp:

```
AC-FS#config
AC-FS(config)#identify-application custom name myxunlei class myp2p udp sport any any dport 200 200
```

3: Configure a user-defined rule, the application category is myqq, the application name is the existing category im in the signature database, the source port is 111, the destination port range is 2020, and the protocol type is udp:

```
AC-FS#config
AC-FS(config)#identify-application custom name myqq class im udp sport 111 111 dport 2020 2020
```

【Verification】 1: Use the show identify-application custom-rule command to display all custom application rules.

【Prompt Information】 1: The ip segment of the configuration rule exceeds 32 ips:

```
AC-FS(config)#identify-application custom name rule1 class TC_AD_KEY tcp dip 172.18.1.20 172.18.
2.255 dport 2 2
High ip address must be larger than low ip address, and the range of ip address can not be larger than
32!
```

2: When ip or port is not allowed to be configured as any, prompt:

```
AC-FS(config)#identify-application custom name rule1 class TC_AD_KEY tcp dip 172.18.1.20 172.18.
2.255 dport any any
It's not allow for either dst ip address or dst port number are "any"!
```

3: When ip or port conflict, prompt:

```
AC-FS(config)#identify-application custom name rule1 class TC_AD_KEY tcp dip 172.18.1.20 172.18.
1.30 dport 2 2
AC-FS(config)#identify-application custom name rule1 class TC_AD_KEY tcp dip 172.18.1.25 172.18.
1.35 dport 2 2
```

Port or ip has already used!

4: When ip or port conflict, prompt:

```
AC-FS#show identify-application custom-rule
TYPE NAME              CLASS        SPL  SPH  DPL  DPH  SIPL SIPH       DIPL    DIPH

TCP rule1              TC_AD_KEY      any any 2   2  any any        172.18.1.20     172.18.1.30
TCP rule2              TC_AD_KEY      any  any  3   20    any any        172.18.1.25 172.18.1.26
TCP rule3              data base                    any any 25   30   any
any        172.18.1.25 172.18.1.25
TCP rule3              data base                     any   any   35   40   any any        172.18.1.25 172.18.1.29
TCP rule3              data base                     any   any   45   50   any any        172.18.1.25 172.18.1.29
TCP rule3              data base                     any   any   55   60   any any        172.18.1.25 172.18.1.29
TCP rule3              data base                    any   any   65   70   any any        172.18.1.25 172.18.1.29
TCP rule3              data base                     any   any   72   72   any any        172.18.1.25 172.18.1.29
TCP rule3              data base                     any   any   74   74   any any        172.18.1.25 172.18.1.29
TCP rule3              data base                    any   any   76   76   any any        172.18.1.25 172.18.1.29
TCP rule3              data base                     any   any   78   78   any any        172.18.1.25 172.18.1.29
TCP rule3              data base                     any   any   80   80   any any        172.18.1.25 172.18.1.29
TCP rule3              data base                     any   any   82   82   any any        172.18.1.25 172.18.1.29
TCP rule3              data base                     any   any   84   84   any any        172.18.1.25 172.18.1.29
TCP rule3              data base                     any   any   86   86   any any        172.18.1.25 172.18.1.29
TCP rule3              data base                     any   any   88   88   any any        172.18.1.25 172.18.1.29
AC-FS(config)# identify-application custom name rule3 class data base tcp dip 172.18 1.25 172.18.1.

29 dport 90 90
The same IP associated with different port cannot exceed 16
```

【Common Mistake】 1: The ip segment of the configuration rule exceeds 32 ips.

2: ip or port is not allowed to be configured as any or both 3: ip or port conflict.

【Platform Description】 Wireless AC series products.

2.8 identify-application dfi enable

Enable dfi's ability to recognize p2p download streams and voice streams.

identify-application dfi enable

Use the no option of this command to turn off application recognition.

no identify-application dfi enable

【Parameter Description】-

【Default Configuration】 It is disabled by default. It can also be turned on separately.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command enables dfi to recognize p2p download streams and voice streams.

【Configuration Example]】1: Enable dfi to recognize p2p and voice streams.

```
AC-FS#config
AC-FS(config)#identify-application dfi enable
```

【Verification】1: Use show running-config to view the function switch. When closed, display:

identify-application dfi enable

【Prompt Information】-

【Common Mistake】-

【Platform Description】 Wireless AC series products.

2.9 identify-application download-group

Add an app to the Download_Group app group.

identify-application download-group app-name

Move an app out of the Download_Group app group.

no identify-application download-group app-name

【Parameter Description】

Parameter	Description
app-name	apply names.

【Default Configuration】Do not join the Download_Group application group by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command can be used to add an application to the Download_Group application group.

【Configuration Example]】1: Add the MSN application to the Download_Group application group.

```
AC-FS#config
AC-FS(config)#identify-application download-group MSN
```

【 Verification 】 1: Use the show identify-application download-group command to view all applications in the Download_Group application group.

【Prompt Information】 1: If an application is already in other system application groups, it will prompt an error. If MSN has already joined the blocking application group, if you add the MSN application to the Download_Group application group, it will prompt:

```
AC-FS(config)#identify-application download-group MSN
The application has already been joined Block_Group!
```

2: If an application that does not exist is added to the Download_Group application group, it will prompt that the application does not exist.

```
AC-FS(config)#identify-application download-group XXX
The application does not exist!
```

【Common Mistake】 1: The application is already in another system application group 2: The application does not exist

【Platform Description】 Wireless AC series products.

2.10 identify-application dpi enable

Enable DPI recognition.

identify-application dpi enable

Turn off DPI recognition.

no identify-application dpi enable

【Parameter Description】-

【Default Configuration】 When application identification is enabled, it is enabled by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to enable the DPI recognition function.

【Configuration Example】1: Enable DPI recognition.

```
AC-FS#config
AC-FS(config)#identify-application dpi enable
```

【Verification】1: Use show running-config to view the function switch. When closed, display:

```
no identify-application dpi enable
```

【Prompt Information】-

【Common Mistake】-

【Platform Description】 Wireless AC series products.

2.11 identify-application enable

Turn on the app-aware global feature.

identify-application enable

Turn off the app-aware global feature.

no identify-application enable

【Parameter Description】-

【Default Configuration】 This function is disabled by default on wireless AC products. In AC virtualization mode, this function cannot be enabled.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Through this command, you can enable the global function of application identification.

【Configuration Example]】1: Enable application recognition.

```
AC-FS#config
AC-FS(config)#identify-application enable
```

【Verification】1: Use show identify-application enable to view the function status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 Wireless AC series products

2.12 identify-application high-group

Add an app to the High_Group app group.

identify-application high-group app-name

Move an app out of the High_Group app group.

no identify-application high-group app-name

【Parameter Description】

Parameter	Description
app-name	Application name.

【Default Configuration】Do not join the High_Group application group by default

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to add an application to the High_Group application group.

【Configuration Example]】1: Add the MSN application to the High_Group application group.

```
AC-FS#config
AC-FS(config)#identify-application high-group MSN
```

【Verification】1: Use the show identify-application high-group command to view all applications in the High_Group application group.

【Prompt Information】 1: If an application is already in other system application groups, it will prompt an error. If MSN has already joined the blocking application group, if you add the MSN application to the High_Group application group, it will prompt:

```
AC-FS(config)#identify-application high-group MSN
The application has already been joined Block_Group!
```

2: If an application that does not exist is added to the High_Group application group, it will prompt that the application does not exist.

```
AC-FS(config)#identify-application high-group XXX
The application does not exist!
```

【Common Mistake】 1: The application is already in another system application group.

2: The application does not exist/

【Platform Description】 Wireless AC series products.

2.13 identify-application inhibitive

Add an app to the Suppressed Apps group.

identify-application inhibitive app-name

Move an app out of the Suppressed Apps group.

no identify-application inhibitive app-name

【Parameter Description】

Parameter	Description
app-name	Application name.

【Default Configuration】 By default, do not join the suppression application group.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command can be used to add an application to the suppression application group.

【Configuration Example]】1: Add the MSN application to the suppression application group.

```
AC-FS#config
AC-FS(config)#identify-application inhibitive MSN
```

【Verification】1: Use the show identify-application inhibitive command to view all applications in the inhibited application group.

【Prompt Information】 1: If an application is already in other system application groups, it will prompt an error. If MSN has been added to the blocking application group, and the MSN application is added to the inhibiting application group, it will prompt:

```
AC-FS(config)#identify-application inhibitive MSN
The application has already been joined Block_Group!
```

2: If an application that does not exist is added to the suppression application group, it will prompt that the application does not exist.

```
AC-FS(config)#identify-application inhibitive XXX
The application does not exist!
```

【Common Mistake】 1: The application is already in another system application group.

2: The application does not exist.

【Platform Description】 Wireless AC series products.

2.14 identify-application key

Add an app to a key app group.

identify-application key app-name

Move an app out of the critical app group.

no identify-application key app-name

【Parameter Description】 -

【Default Configuration】 The key application group is not added by default

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command can be used to add an application to the key application group.

【Configuration Example]】 1: Add MSN applications to key application groups.

```
AC-FS#config
AC-FS(config)#identify-application key MSN
```

【Verification】 1: Use the show identify-application key command to view all applications in the key application group.

【Prompt Information】 1: If an application is already in other system application groups, it will prompt an error. If MSN has been added to the blocking application group, and the MSN application is added to the key application group, it will prompt:

```
AC-FS(config)#identify-application key MSN
The application has already been joined Block_Group!
```

2: If an application that does not exist is added to the key application group, it will prompt that the application does not exist.

```
AC-FS(config)#identify-application key XXX
The application does not exist!
```

【Common Mistake】 1: The application is already in another system application group.

2: The application does not exist.

【Platform Description】 Wireless AC series products.

2.15 identify-application len-seq enable

Turn on the length sequence recognition function.

identify-application len-seq enable

Turn off length sequence recognition.

no identify-application len-seq enable

【Parameter Description】-

【Default Configuration】 When application identification is enabled, it is enabled by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to enable length sequence recognition.

【Configuration Example】1: Enable length sequence recognition.

```
AC-FS#config
AC-FS(config)#identify-application len-seq enable
```

【Verification】1: Use show running-config to view the function switch. When closed, display:

```
no identify-application len-seq enable
```

【Prompt Information】-

【Common Mistake】-

【Platform Description】 Wireless AC series products

2.16 identify-application low-group

Add an app to the Low_Group app group.

identify-application low-group app-name

Move an app out of the Low_Group app group.

no identify-application low-group app-name

【Parameter Description】

Parameter	Description
app-name	Application name.

【Default Configuration】Do not join the Low_Group application group by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command can be used to add an application to the Low_Group application group.

【Configuration Example]】1: Add the MSN application to the Low_Group application group.

```
AC-FS#config
AC-FS(config)#identify-application low-group MSN
```

【Verification】1: Use the show identify-application low-group command to view all applications in the Low_Group application group.

【Prompt Information】 1: If an application is already in other system application groups, it will prompt an error. If MSN has been added to the blocking application group, and the MSN application is added to the Low_Group application group, it will prompt:

```
AC-FS(config)#identify-application low-group MSN
The application has already been joined Block_Group!
```

2: If an application that does not exist is added to the Low_Group application group, it will prompt that the application does not exist.

```
AC-FS(config)#identify-application low-group XXX
The application does not exist!
```

【Common Mistake】 1: The application is already in another system application group.

2: The application does not exist.

【Platform Description】 Wireless AC series products.

2.17 identify-application middle-group

Add an app to the Middle_Group app group.

identify-application middle-group app-name

Move an app out of the Middle_Group app group.

no identify-application middle-group app-name

【Parameter Description】-

【Default Configuration】 Do not join the Middle_Group application group by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to add an application to the Middle_Group application group.

【Configuration Example]】 1: Add the MSN application to the Middle_Group application group.

```
AC-FS#config
AC-FS(config)#identify-application middle-group MSN
```

【Verification】 1: Use the show identify-application middle-group command to view all applications in the Middle_Group application group.

【Prompt Information】 1: If an application is already in other system application groups, it will prompt an error. If MSN has already joined the blocking application group, if you add the MSN application to the Middle_Group application group, it will prompt:

```
AC-FS(config)#identify-application middle-group MSN
The application has already been joined Block_Group!
```

2: If an application that does not exist is added to the Middle_Group application group, it will prompt that the application does not exist.

```
AC-FS(config)#identify-application middle-group XXX
The application does not exist!
```

【Common Mistake】 1: The application is already in other system application groups.

2: Application does not exist.

【Platform Description】 Wireless AC series products.

2.18identify-application online-video-group

Add an app to the Online_Video_Group app group.

identify-application online-video-group app-name

Move an app out of the Online_Video_Group app group.

no identify-application online-video-group app-name

【Parameter Description】

Parameter	Description
app-name	Application name.

【Default Configuration】 Do not join the Online_Video_Group application group by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command can be used to add an application to the Online_Video_Group application group.

【Configuration Example]】 1: Add the MSN application to the Online_Video_Group application group.

```
AC-FS#config
AC-FS(config)#identify-application online-video-group MSN
```

【Verification】 1: Use the show identify-application online-video-group command to view all applications in the Online_Video_Group application group.

【Prompt Information】 1: If an application is already in other system application groups, it will prompt an error. If MSN has already joined the blocking application group, if you add the MSN application to the Online_Video_Group application group, it will prompt:

```
AC-FS(config)#identify-application online-video-group MSN
The application has already been joined Block_Group!
```

2: If an application that does not exist is added to the Online_Video_Group application group, it will prompt that the application does not exist.

```
AC-FS(config)#identify-application online-video-group XXX
The application does not exist!
```

【Common Mistake】 1: The application is already in another system application group.

2: The application does not exist.

【Platform Description】 Wireless AC series products.

2.19 identify-application other

Add an app to another app group.

identify-application other app-name

Move an app out of another app group.

no identify-application other app-name

【Parameter Description】

Parameter	Description
app-name	Application name.

【Default Configuration】 Add to other application groups by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command can be used to add an application to other application groups.

【Configuration Example]】1: Add MSN applications to other application groups.

```
AC-FS#config
AC-FS(config)#identify-application other MSN
```

【Verification】1: Use the show identify-application other command to view all applications in other application groups.

【Prompt Information】 1: If an application that does not exist is added to another application group, it will prompt that the application does not exist.

```
AC-FS(config)#identify-application other XXX
The application does not exist!
```

【Common Mistake】 1: The application does not exist.

【Platform Description】 Wireless AC series products.

2.20 identify-application p2p-group

Add an app to the P2p_Group app group.

identify-application p2p-group app-name

Move an app out of the P2p_Group app group.

no identify-application p2p-group app-name

【Parameter Description】

Parameter	Description
app-name	Application name.

【Default Configuration】Do not join the P2p_Group application group by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command can be used to add an application to the P2p_Group application group.

【Configuration Example]】1: Add the MSN application to the P2p_Group application group.

```
AC-FS#config
AC-FS(config)#identify-application p2p-group MSN
```

【Verification】1: Use the show identify-application p2p-group command to view all applications in the P2p_Group application group.

【Prompt Information】1: If an application is already in other system application groups, it will prompt an error. If MSN has been added to the blocking application group, and the MSN application is added to the P2p_Group application group, it will prompt:

```
AC-FS(config)#identify-application p2p-group MSN
The application has already been joined Block_Group!
```

2: If an application that does not exist is added to the P2p_Group application group, it will prompt that the application does not exist.

```
AC-FS(config)#identify-application p2p-group XXX
The application does not exist!
```

【Common Mistake】 1: The application is already in another system application group.

2: The application does not exist.

【Platform Description】 Wireless AC series products.

2.21 identify-application p2p-video-group

Add an app to the P2p_Video_Group app group.

identify-application p2p-video-group app-name

Move an app out of the P2p_Video_Group app group.

no identify-application p2p-video-group app-name

【Parameter Description】

Parameter	Description
app-name	Application name.

【Default Configuration】Do not join the P2p_Video_Group application group by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command can be used to add an application to the P2p_Video_Group application group.

【Configuration Example]】1: Add the MSN application to the P2p_Video_Group application group.

```
AC-FS#config
AC-FS(config)#identify-application p2p-video-group MSN
```

【 Verification 】 1: Use the show identify-application p2p-video-group command to view all applications in the P2p_Video_Group application group.

【Prompt Information】 1: If an application is already in other system application groups, it will prompt an error. If MSN has been added to the blocking application group, and the MSN application is added to the P2p_Video_Group application group, it will prompt:

```
AC-FS(config)#identify-application p2p-video-group MSN
The application has already been joined Block_Group!
```

2: If an application that does not exist is added to the P2p_Video_Group application group, it will prompt that the application does not exist.

```
AC-FS(config)#identify-application p2p-video-group XXX
The application does not exist!
```

【Common Mistake】 1: The application is already in another system application group.

2: The application does not exist.

【Platform Description】 Wireless AC series products

2.22 identify-application proto-detect enable

Enable the application identification protocol detection and identification function.

identify-application proto-detect enable

Use the no option of this command to turn off the protocol probe identification function.

no identify-application proto-detect enable

【Parameter Description】-

【Default Configuration】 This function is enabled by default when app recognition is enabled.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to enable the protocol expected recognition function.

【Configuration Example]】1: Enable the protocol expectation recognition function.

```
AC-FS#config
AC-FS(config)# identify-application proto-detect enable
```

【Verification】1: Use show running-config to view the function switch. When closed, display:

no identify-application proto-expect enable

【Prompt Information】-

【Common Mistake】-

【Platform Description】 Wireless AC series products.

2.23 identify-application proto-expect enable

Enable the application identification protocol expected identification function.

identify-application proto-expect enable

Use the no option of this command to turn off protocol-expected recognition.

no identify-application proto-expect enable

【Parameter Description】-

【Default Configuration】 This function is enabled by default when app recognition is enabled.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to enable the protocol expected recognition function.

【Configuration Example]】1: Enable the protocol expectation recognition function.

```
AC-FS#config
AC-FS(config)# identify-application proto-expect enable
```

【Verification】1: Use show running-config to view the function switch. When closed, display:

no identify-application proto-expect enable

【Prompt Information】-

【Common Mistake】-

【Platform Description】 Wireless AC series products.

2.24 identify-application proto-expect timeout

Configure the aging time of the nodes expected by the protocol.

identify-application proto-expect timeout time-seconds

Unconfigure the protocol's expected node aging time.

no identify-application proto-expect timeout

【Parameter Description】

Parameter	Description
time-seconds	Number of seconds for aging, Parameter range 10-3600.

【Default Configuration】 The default parameter is 60 seconds.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Through this command, you can configure the expected aging time of the protocol node.

【Configuration Example]】1: The aging time of the node expected by the configuration protocol is 3 minutes.

```
AC-FS#config
AC-FS(config)# identify-application proto-expect timeout 180
```

【Verification】1: Use show running-config to view. When configured, display

identify-application proto-expect timeout 180

【Prompt Information】-

【Common Mistake】-

【Platform Description】 Wireless AC series products.

2.25 identify-application signature update

Upgrade the signature library.

identify-application signature update

【Parameter Description】-

【Default Configuration】 By default, the system will be automatically upgraded after one minute of startup.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command can be used to upgrade and update the signature database.

【Configuration Example]】1: Download the latest signature library version from the link provided on the WEB upgrade interface.

2: After decompression, download the signature library to the device through tftp.

```
AC-FS#copy tftp://172.18.3.11/app_signature.upd flash:app_signature.upd
Accessing tftp://172.18.3.11/app_signature.upd...
!!!!!!!!!!!!!!!!
Transmission finished, file length 242952  bytes.

Download file [app_signature.upd] to file system is OK.
AC-FS#run-system-shell
~ # cp /data/app_signature.upd /sbin/signature/app_tmp/
~ # exit AC-
FS#
```

3: Upgrade the signature database.

```
AC-FS#config
AC-FS(config)# identify-application signature update
```

【Verification】 1: Use show identify-application version to view the signature library version information.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 Wireless AC series products.

2.26 identify-application update-group

Add an app to the Update_Group app group.

identify-application update-group app-name

Move an app out of the Update_Group app group.

no identify-application update-group app-name

【Parameter Description】

Parameter	Description
app-name	Application name.

【Default Configuration】 Do not join the Update_Group application group by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to add an application to the Update_Group application group.

【Configuration Example]】1: Add the MSN application to the Update_Group application group.

```
AC-FS#config
AC-FS(config)#identify-application update-group MSN
```

【Verification】1: Use the show identify-application update-group command to view all applications in the Update_Group application group.

【Prompt Information】1: If an application is already in other system application groups, it will prompt an error. If MSN has been added to the blocking application group, and the MSN application is added to the Update_Group application group, it will prompt:

```
AC-FS(config)#identify-application update-group MSN
The application has already been joined Block_Group!
```

2: If an application that does not exist is added to the Update_Group application group, it will prompt that the application does not exist.

```
AC-FS(config)#identify-application update-group XXX
The application does not exist!
```

【Common Mistake】 1: The application is already in other system application groups.

2: Application does not exist.

【Platform Description】 Wireless AC series products.

2.27 identify-application upload-group

Add an app to the Upload_Group app group.

identify-application upload-group app-name

Move an app out of the Upload_Group app group.

no identify-application upload-group app-name

【Parameter Description】

Parameter	Description
app-name	Application name.

【Default Configuration】 Do not join the Upload_Group application group by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command can be used to add an application to the Upload_Group application group.

【Configuration Example]】 1: Add the MSN application to the Upload_Group application group.

```
AC-FS#config
AC-FS(config)#identify-application upload-group MSN
```

【Verification】 1: Use the show identify-application upload-group command to view all applications in the Upload_Group application group.

【Prompt Information】 1: If an application is already in other system application groups, it will prompt an error. If MSN has already joined the blocking application group, if you add the MSN application to the Upload_Group application group, it will prompt:

```
AC-FS(config)#identify-application upload-group MSN
The application has already been joined Block_Group!
```

2: If an application that does not exist is added to the Upload_Group application group, it will prompt that the application does not exist.

```
AC-FS(config)#identify-application upload-group XXX
The application does not exist!
```

【Common Mistake】 1: The application is already in another system application group.

2: The application does not exist.

【Platform Description】 Wireless AC series products.

2.28 identify-application web-group

Add an application to the Web_Group application group.

identify-application web-group app-name

Move an app out of the Web_Group app group.

no identify-application web-group app-name

【Parameter Description】

Parameter	Description
app-name	Application name.

【Default Configuration】 Do not join the Web_Group application group by default

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 This command can be used to add an application to the Web_Group application group.

【Configuration Example]】 1: Add the MSN application to the Web_Group application group.

```
AC-FS#config
AC-FS(config)#identify-application web-group MSN
```

【Verification】 1: Use the show identify-application web-group command to view all applications in the Web_Group application group.

【Prompt Information】 1: If an application is already in other system application groups, it will prompt an error. If MSN has been added to the blocking application group, and the MSN application is added to the Web_Group application group, it will prompt:

```
AC-FS(config)#identify-application web-group MSN
The application has already been joined Block_Group!
```

2: If an application that does not exist is added to the Web_Group application group, it will prompt that the application does not exist.

```
AC-FS(config)#identify-application web-group XXX
The application does not exist!
```

【Common Mistake】 1: The application is already in another system application group.

2: The application does not exist.

【Platform Description】 Wireless AC series products.

2.29 show identify-application

Displays application rule tree information.

show identify-application

【Parameter Description】-

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】-

【Usage Guide】 This command can print out the information of the current application rule tree.

【Configuration Example]】1: Display application rule tree information.

```
AC-FS#show identify-application any 255-4095-63-48
  Instant messaging software 1-0-0-0
    Ali Wangwang 1-1-0-0
    MSN 1-6-0-0
      MSN-CHAT 1-6-1-0
      MSN-AUDIO 1-6-2-0
      MSN-FILE 1-6-3-0
      MSN-video 1-6-4-0
      MSN- log on 1-6-5-0
    TencentQQ 1-7-0-0
      QQ-CHAT 1-7-1-0
      QQ-voice 1-7-2-0
      QQ-file transfer1-7-3-0
      QQ-File sharing 1-7-4-0
      QQ-video 1-7-5-0
      QQ-log on 1-7-14-0
    WEBIM 1-9-0-0
      MSN-WEBIM 1-9-1-0
      YAHOO-WEBIM 1-9-2-0
      AIM 1-9-3-0
    Netease bubble 1-12-0-0
    Feixin 1-14-0-0
  IP Internet telephone 2-0-0-0
    SKYPE 2-7-0-0
    h232 protocol family 2-12-0-0

H323-HOSTCALLSC 2-12-4-0
CALL-SIG-TRANS 2-12-5-0
RTCP 2-12-6-0
RTP 2-12-7-0
IMTC-MCS 2-12-10-0
```

【Prompt Information】-

【Platform Description】 Wireless AC series products.

2.30 show identify-application block

Displays the apps or categories that are added to the blocking app group.

show identify-application block

【Parameter Description】

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Through this command, you can view which applications or categories have joined the blocking application group.

【Configuration Example]】1: Display the applications in the blocking application group.

```
AC-FS# show identity-application block
```

【Prompt Information】-

【Platform Description】 Wireless AC series products.

2.31 show identify-application class

Displays application classification information.

show identify-application class [class-name]

【Parameter Description】

Parameter	Description
class-name	Application name.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to view application category information, or applications under a certain application category.

【Configuration Example]】1: View application categories

```
AC-FS# show identify-application class
Instant messaging software  1-0-0-0
IP Internet telephone
2-0-0-0
Online game software
3-0-0-0
Video streaming software
4-0-0-0 P2P
Application software  5-0-0-0
Stock software 6-0-0-0
WEB Application 7-0-0-0 HTTP Game 38-0-0-0
Internet file transfer 8-0-0-0
Email protocol  9-0-0-0
database 10-0-0-0
Network management protocol
11-0-0-0
Routing protocol 12-0-0-0
Security protocol 13-0-0-0 VPN
Application 14-0-0-0
Remote access protocol
 15-0-0-0
Software update   17-0-0-0 HTTP
Video 18-0-0-0
Online banking 19-0-0-0
Network hard disk 20-0-0-0
instant messaging_MOBILE 21-0-0-0 Video | video and audio_MOBILE
22-0-0-0
Download tools_MOBILE 23-0-0-0
Game_MOBILE 24-0-0-0
```

2: View applications under an application category.

```
AC-FS# show identify-application class Internet file transfer
FTP 8-4-0-0 HTTPS 8-7-0-0 NNTP 8-12-0-0
TFTP 8-16-0-0
```

```
IXIA 8-17-0-0 SVN 8-18-0-0 SMB 8-21-0-0
HFS 8-22-0-0
```

【Prompt Information】-

【Platform Description】 Wireless AC series products

2.32 show identify-application custom-group

Displays application grouping information.

show identify-application custom-group

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 All applications can be grouped by this command.

【Configuration Example]】1: View application groups.

```
AC-FS# show identify-application custom-group system-group: Key_Group
system-group: Unkey_Group system-group: Block_Group
  application: MSN (group) system-group: Other_Group
  application: Instant messaging software (group)
  application: IP Internet telephone (group)
  application: Online game software (group)
  application: Video streaming software (group)
  application: P2P application software (group)
  application: Stock software (group)
  application: Web application (group)
  application: HTTP Game (group)
  application: Internet file transfer (group)
  application: Email protocol (group)
  application: database (group)
```

application: Network management protocol (group)
application: Routing protocol (group)
application: Security protocol (group)
application: VPN application (group)
application: Remote access protocol (group)
application: Software update (group)
application: HTTP video (group)
application: Online banking (group)
application: Network hard disk (group)
application: instant messaging_MOBILE (group)
application: Video | video and audio_MOBILE (group)
application: Download tools_MOBILE (group)
application: Game_MOBILE (group)
application: social contact_MOBILE (group)
application: Net disk_MOBILE (group)
application: WEB_MOBILE (group)
application: other_MOBILE (group)
application: online shopping_MOBILE (group)
application: stock_MOBILE (group)
application: Online payment | online banking_MOBILE (group)
application: micro-blog(group)
application: office OA (group)
application: Videoconferencing (group)
application: HTTP downloads (group)
application: HTTP uploads (group)
application: RFC (group)
application: ICMP-DETAIL (group)
application: IP-RAW (group)
application: IP Protocol group (group)
application: TC_AD_KEY (group) custom-group: TC_AD_Key
application: WEB application (group)
application: HTTP downloads (group)
application: P2P-HTTP downloads
application: Download tools_MOBILE (group) custom-group: route~route
application: WEB application (group)
application: HTTP downloads (group)
application: HTTP uploads (group) custom-group: 1~route
application: HTTP downloads (group)
Anwendung: http upload (Gruppe)

【Prompt Information】-

【Platform Description】 Wireless AC series products

2.33 show identify-application custom-rule

Displays custom application rules.

show identify-application custom-rule

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 All application rules can be customized by this command.

【Configuration Example]】1: View application groups.

```
AC-FS# show identify-application custom- rule
TYPE NAME                    CLASS                    SPL   SPH   DPL   DPH   SIPL
SIPH                       DIPL                     DIPH
____ ______________________ ________________________ ____ ____ ____ ____
_______________________ _______________________ _______________________
_______________________

tcp  111                     222                      any  any  any   any
1.1.1.1                    1.1.1.1.................2.2.2.2
2.2.2.2
tcp  444                     222                      any  any  any   any
3.3.3.3                    3.3.3.3                  4.4.4.4
4.4.4.4
tcp  333                     222                      any any any any
2001:333:444:555::2        2001:333:444:555::1f     2400:111:222:333::ff01
2400:111:222:333::ff1a
```

Field Description:

Field	Description
TYPE	Protocol information.
NAME	Rule name.

CLASS	Application classification to which the rule belongs.
SPL	Start source port.
SPH	Terminate source port.
DPL	Start destination port.
DPH	Terminate destination port.
SIPL	Starting source IP address.
SIPH	Terminate source IP address.
DIPL	Start destination IP address.
DIPH	Termination destination IP address.

【Prompt Information】-

【Platform Description】 Wireless AC series products.

2.34 show identify-application dfi enable

Check out the Application Recognition DFI feature.

show identify-application dfi enable

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Through this command, you can view the application recognition DFI function.

【Configuration Example]】1: View application recognition DFI function.

```
AC-FS# show identify-application dfi enable
dfi enable!
```

【Prompt Information】-

【Platform Description】 Wireless AC series products.

2.35 show identify-application download-group

Displays apps or categories added to the Download_Group app group.

show identify-application download-group

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Through this command, you can view which applications or categories are currently added to the Download_Group application group.

【Configuration Example]】1: Display the applications in the Download_Group application group.

```
AC-FS# show identity-application download-group
MSN
QQ
```

【Prompt Information】-

【Platform Description】 Wireless AC series products.

2.36 show identify-application enable

Check out the app recognition feature.

show identify-application enable

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to view the application identification function.

【Configuration Example]】1: View the application identification function.

```
AC-FS# show identify-application enable
on
```

【Prompt Information】-

【Platform Description】 Wireless AC series products.

2.37 show identify-application group-state

Display grouping mode.

show identify-application group-state

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to view the current grouping mode.

【Configuration Example]】1: Display application classification information:

```
AC-FS#show identity-application group-state
app group state: on
```

Field Description:

Field	Description
app group state	On the current application is divided into key application groups, inhibited application groups, and IP collaboration groups. The panel is divided into groups.

【Prompt Information】-

【Platform Description】 Wireless AC series products

2.38 show identify-application high-group

Displays apps or categories that are part of the High_Group app group.

show identify-application high-group

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Through this command, you can view which applications or categories are currently added to the High_Group application group.

【Configuration Example]】1: Display applications in the High_Group application group.

```
AC-FS# show identity-application high-group
MSN
QQ
```

【Prompt Information】-

【Platform Description】 Wireless AC series products.

2.39 show identify-application inhibitive

Displays the apps or categories that are added to the suppressed app group.

show identify-application inhibitive

【Parameter Description】

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Through this command, you can view which applications or categories are currently added to the suppression application group.

【Configuration Example]】1: Display and suppress applications in the application group.

```
AC-FS# show identity-application inhibitive
Stock software
Baidu down
Thunder
```

【Prompt Information】-

【Platform Description】 Wireless AC series products.

2.40show identify-application key

Displays apps or categories that are added to key app groups.

show identify-application key

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Through this command, you can view which applications or categories have joined the key application group.

【Configuration Example]】1: Display applications in key application groups.

```
AC-FS# show identity-application key
MSN
QQ
```

【Prompt Information】-

【Platform Description】 Wireless AC series products.

2.41 show identify-application low-group

Displays apps or categories that are added to the Low_Group app group.

show identify-application low-group

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【 Usage Guide 】 Through this command, you can view which applications or categories are currently added to the Low_Group application group.

【Configuration Example]】1: Display applications in the Low_Group application group.

```
AC-FS# show identity-application low-group
MSN
QQ
```

【Prompt Information】-

【Platform Description】 Wireless AC series products.

2.42show identify-application middle-group

Displays apps or categories that are added to the Middle_Group app group.

show identify-application middle-group

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【 Usage Guide 】 Through this command, you can view which applications or categories are currently added to the Middle_Group application group.

【Configuration Example]】1: Display applications in the Middle_Group application group.

```
AC-FS# show identity-application middle-group
MSN
QQ
```

【Prompt Information】-

【Platform Description】 Wireless AC series products.

2.43 show identify-application online-video-group

Displays apps or categories that are part of the Online_Video_Group app group.

show identify-application online-video-group

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Through this command, you can view which applications or categories are currently added to the Online_Video_Group application group.

【Configuration Example]】1: Display the applications in the Online_Video_Group application group.

```
AC-FS# show identity-application online-video-group
MSN
QQ
```

【Prompt Information】-

【Platform Description】 Wireless AC series products.

2.44 show identify-application other

Displays applications or categories of other application groups.

show identify-application other

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Through this command, you can view the current applications or categories that have joined other application groups.

【Configuration Example]】1: Display applications in other application groups.

```
AC-FS# show identity-application other
MSN
QQ
```

【Prompt Information】-

【Platform Description】 Wireless AC series products.

2.45 show identify-application p2p-group

Displays apps or categories added to the P2p_Group app group.

show identify-application p2p-group

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Through this command, you can view which applications or categories are currently added to the P2p_Group application group.

【Configuration Example]】1: Display applications in the P2p_Group application group.

```
AC-FS# show identity-application p2p-group
MSN
QQ
```

【Prompt Information】-

【Platform Description】 Wireless AC series products.

2.46 show identify-application p2p-video-group

Displays apps or categories added to the P2p_Video_Group app group.

show identify-application p2p-video-group

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Through this command, you can view which applications or categories are currently added to the P2p_Video_Group application group.

【Configuration Example]】1: Display applications in the P2p_Video_Group application group.

```
AC-FS# show identity-application p2p-video-group
MSN
QQ
```

【Prompt Information】-

【Platform Description】 Wireless AC series products.

2.47 show identify-application proto-expect enable

Displays information expected by the protocol.

show identify-application proto-expect enable

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to view the current protocol expected information.

【Configuration Example】1: Display the expected basic information of the protocol.

```
AC-FS#show identify-application proto-expect enable
Proto-expect is enable
Proto-expect app_db is unable
Proto-expect timeout is not set[0s]
```

【Prompt Information】-

【Platform Description】 Wireless AC series products.

2.48 show identify-application proto-detect enable

Displays information about protocol probes.

show identify-application proto-detect enable

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to view the current protocol detection information.

【Configuration Example】1: Display the expected basic information of the protocol.

```
AC-FS#show identify-application proto-detect enable
proto-detect is on
```

【Prompt Information】-

【Platform Description】 Wireless AC series products.

2.49 show identify-application update-group

Displays apps or categories added to the Update_Group app group.

show identify-application update-group

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Through this command, you can view which applications or categories are currently added to the Update_Group application group.

【Configuration Example]】1: Display applications in the Update_Group application group.

```
AC-FS# show identity-application update-group
MSN
QQ
```

【Prompt Information】-

【Platform Description】 Wireless AC series products.

2.50 show identify-application upload-group

Displays apps or categories added to the Upload_Group app group.

show identify-application upload-group

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Through this command, you can view which applications or categories are currently added to the Upload_Group application group.

【Configuration Example]】1: Display the applications in the Upload_Group application group

```
AC-FS# show identity-application upload-group
MSN
QQ
```

【Prompt Information】-

【Platform Description】 Wireless AC series products.

2.51 show identify-application version

Displays the version number information of the signature library.

show identify-application version

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to view the current signature library version information.

【Configuration Example]】1: View the current signature library version information.

```
AC-FS# show identify-application version
Version:2013.06.10.13.06.10(V2.0)
```

Field Description:

field	Description
Version	version number.

【Prompt Information】-

【Platform Description】 Wireless AC series products

2.52 show identify-application web-group

Displays apps or categories that are added to the Web_Group app group.

show identify-application web-group

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【 Usage Guide 】 Through this command, you can view which applications or categories are currently added to the Web_Group application group.

【Configuration Example]】1: Display the applications in the Web_Group application group.

```
AC-FS# show identity-application web-group
MSN
QQ
```

【Prompt Information】-

【Platform Description】 Wireless AC series products.

3 Global session limit

3.1 flow-pre-mgr { down-deny | down-permit }

Filter new upstream packets

flow-pre-mgr { down -deny | down -permit } id { { { ip | icmp | ospf } { src-host { ip-addr | any } | src-range { ip-start ip-end | any } | src-subnet { ip-subnet ip-mask | any } } { dst-host ip-addr | dst-range ip-start ip-end | dst-subnet ip-subnet ip-mask } } | { { { tcp | udp } { src-host { ip-addr | any } | src-range { ip-start ip-end | any } | src-subnet { ip -subnet ip-mask | any } } { src-port { port | any } | sport-range { port-srart port-end | any } } { dst-host ip-addr | dst-range ip-start ip-end | dst-subnet ip-subnet ip-mask } { dst-port { port | any } | dport-range { port-srart port-end | any } } } }

Delete a filter rule

no flow-pre-mgr { down-deny | down-permit } id

【Parameter Description】

Parameter	Description
ip-addr	The specific IP as specified.
ip-start	Specifies the start IP for the IP range.
ip-end	Specifies the end IP for the IP range.
ip-subnet	Specifies the subnetwork segment.
ip-mask	Specifies the mask.
port	port.
port-srart	Start port of the port range.
port-end	End port of the port range.

【Default Configuration】 No configuration

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 The function and ip session filter are both used for packet filtering, but the performance of the two is different. If the configured ACL has a large number of ACEs, it is recommended to use this command, and the performance will be improved. This command is used to filter downlink construction packets, and is matched with the command to filter uplink construction packets.

When configuring the upstream new packet filtering rule, the source IP cannot be any. When configuring a new downlink packet filtering

rule, the destination IP address should not be any. Permit and deny rules have their own IDs and will not conflict.

Deny rules take precedence over permit rules.

【Configuration Example]】 The configuration does not allow the external network to access all ports of the device except port 80, and prohibit the external network IP 110.110.110.24 from pinging the device. Device IP172.18.124.118.

```
AC-FS# configure terminal
AC-FS(config)# flow-pre-mgr down-deny 1 icmp src-host 110.110.110.24 dst-host 172.18.124.118 AC-
FS(config)# flow-pre-mgr down-permit 1 tcp src-host any src-port any dst-host 172.18.124.118 dst-
port 80
AC-FS(config)# flow-pre-mgr down-permit 2 udp src-host any src-port any dst-host 172.18.124.118
dst-port 80
```

【Verification】 1. Use show flow-pre-mgr drop-count to check the packet loss.

2. Use show ip session filter to view the number of packets matched by each rule.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

3.2 flow-pre-mgr { up-deny | up-permit }

Filter new upstream packets.

flow-pre-mgr { up-deny | up-permit } id { { { ip | icmp | ospf } { src-host ip-addr | src-range ip-start ip-end | src-subnet ip-subnet ip-mask } { dst-host { ip-addr | any } | dst-range { ip-start ip-end | any } | dst-subnet { ip-subnet ip-mask | any } } } | { { tcp | udp } { src-host ip-addr | src-range ip-start ip-end | src-subnet ip-subnet ip-mask } { src- port { port | any } | sport-range { port-srart port-end | any } } { dst-host {ip-addr | any} | dst-range { ip-start ip-end | any } | dst-subnet { ip-subnet ip-mask | any } } { dst-port { port | any } | dport-range { port-srart port-end | any } } } }

Delete a filter rule.

no flow-pre-mgr { up-deny | up-permit } id

【Parameter Description】

Parameter	Description
ip-addr	The specific IP as specified.
ip-start	Specifies the start IP for the IP range.
ip-end	Specifies the end IP for the IP range.
ip-subnet	Specifies the subnetwork segment.
ip-mask	Specifies the mask.
port	Port.
port-srart	Start port of the port range.
port-end	End port of the port range.

【Default Configuration】 No configuration

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 The function and ip session filter are both used for packet filtering, but the performance of the two is different. If the configured ACL has a large number of ACEs, it is recommended to use this command, and the performance will be improved. This command is used to filter the upstream construction packets, and is matched with the command to filter the downstream newly constructed packets.

When configuring the upstream new packet filtering rule, the source IP cannot be any. When configuring a new downlink packet filtering rule, the destination IP address should not be any. Permit and deny rules have their own IDs and will not conflict.

Deny rules take precedence over permit rules.

【Configuration Example]】The configuration allows the IP of the intranet 192.168.1.0/24 network segment and the 172.18.1.0/24 network shield to access the Internet, but prohibits the 192.168.1.24 IP from accessing the Internet.

```
AC-FS# configure terminal
AC-FS(config)# flow-pre-mgr up-deny 1 ip src-host 192.168.1.24 dst-host any
AC-FS(config)# flow-pre-mgr up-permit 1 ip src-subnet 192.168.1.0 255.255.255.0 dst-host any AC-FS(config)# flow-pre-mgr
up-permit 2 ip src-subnet 172.18.1.0 255.255.255.0 dst-host any
```

【Verification】 3. Use show flow-pre-mgr drop-count to check the packet loss.

4. Use show ip session filter to view the number of packets matched by each rule.

【Prompt Information】 -

【Common Mistake】-

【Platform Description】 -

3.3 flow-pre-mgr access-list

Configure ACL-based session limit value

flow-pre-mgr rule-id access-list acl-number action { block | by-pass | { trust total-limit total-limit-number } }

Delete an ACL-based session limit rule

no flow-pre-mgr rule-id

【Parameter Description】

Parameter	Description
rule-id	The identification number of the rule, the value range is 1~50. When the configured identification number has been used, a conflict will be displayed and the configuration cannot be successful.
acl-number	The ACL number associated with the rule, with values ranging from 1 to 199.
total-limit total-limit-number	ACL total flow session limit value, the value range is related to device memory, where 0 indicates no limit.

【Default Configuration】 No related configuration

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 1. Configure the ACL-based flow session number control mode: block, by-pass or trust. To delete the related configuration, execute no flow-pre-mgr id in the global configuration mode.

2. The configured rules have priority, and the priority is defined according to the principle that the last configured rule has the highest priority.

3. ACL-based flow session limit does not allow users to configure the limit of flow sessions per IP.

4. Description of action, block means that flow session communication is not allowed; by-pass means that there is no need to create a flow session, and the message is forwarded directly according to the mapping relationship of the bridge (this command keyword only appears

in bridge mode and one-arm mode. , there is no such command keyword in gateway mode); trust indicates the limit of the total number of flow sessions allowed to configure the ACL. After the flow session exceeds the specified limit value, the new flow session communication will not be allowed.

5. The source IP in the ACL corresponds to the internal network IP, the source port corresponds to the internal network port, the destination IP corresponds to the external network IP, and the destination port corresponds to the external network port.

6. The maximum number of streaming sessions that the device can support is related to the device's memory. When configuring this command, the maximum allowable input is the maximum number of streaming sessions supported by the device.

7. The ACL-based flow session limit rule has a great impact on performance and cannot be configured too much. This rule is usually used to prevent devices from creating meaningless streaming sessions, see examples.

8. For the ACL associated with the rule, the ACL entry contained in it only supports the configuration of source IP, source port, destination IP, destination port, and protocol number, otherwise the ACL entry cannot take effect in this module.

9. In gateway mode, we do not limit the source-to-source data flow caused by the routing error of the upper-level router.

ACLs must be configured first.

【Configuration Example】 1. Configure an ACL to match the flow established between the device and the external network IP: 220.200.20.20, and limit the number of flow sessions to 30.

```
AC-FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z. AC-
FS(config)#ip access-list extended 120
AC-FS(config-ext-nacl)#permit ip any host 220.220.20.20
AC-FS(config-ext-nacl)#deny ip any any
AC-FS(config-ext-nacl)#exit
AC-FS(config)#flow-pre-mgr 2 access-list 120 action trust total-limit 30
```

2. Assuming that the intranet IP segment is 192.168.1.0/24, our requirement is that except the IP of the intranet segment needs to create a streaming session, the rest are processed by-pass.

```
AC-FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z. AC-
FS(config)#ip access-list standard 2
AC-FS(config-std-nacl)#deny 192.168.1.0 0.0.0.255
AC-FS(config-std-nacl)#permit any
AC-FS(config-ext-nacl)#exit
AC-FS(config)# flow-pre-mgr 1 access-list 1 action by-pass
```

【Verification】 1. Use show flow-pre-mgr rule-info to view the configured rules and session matching;

2. Use show flow-pre-mgr ip-info to view IP sessions and restrictions.

【Prompt Information】 1: If the rule ID has been used, it will prompt an error.

Rule id already exists, please delete it first

【Common Mistake】 The specified ACL is not configured.

【Platform Description】 -

3.4 flow-pre-mgr enable

Enable global session limit function.

flow-pre-mgr enable

Turn off the global session limit function.

no flow-pre-mgr enable

【Parameter Description】-

【Default Configuration】 Open state

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Use this command to enable the global session limit function. The default switch is enabled. Use no flow-pre-mgr enable to disable the global session count feature.

【Configuration Example]】Disable the global session limit function.

```
AC-FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z. AC-
FS(config)# no flow-pre-mgr enable
```

【Verification】Use show running-config to check whether there is no flow-pre-mgr enable, if not, it is enabled.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.5flow-pre-mgr new-session-limit { specify | specify-range | specify-subnet }

After configuring the new connection limit for real IP, some special IPs (such as servers) may need to relax the limit value.

flow-pre-mgr new-session-limit { specify ip-addr | specify-range ip-start ip-end | specify-subnet ip-subnet ip-mask } limit limit-number

Remove new connection limit specifying real IP

no flow-pre-mgr new-session-limit { specify ip-addr | specify-range ip-start ip-end | specify-subnet ip-subnet ip-mask }

【Parameter Description】

Parameter	Description
ip-addr	Specified specific IP.
ip-start	Specifies the start IP of the IP range.
ip-end	Specifies the end IP of the IP range.
ip-subnet	Specify subnet segment.
ip-mask	Specify mask.
limit-number	Uplink packet speed limit, value range: 0-100000.

【Default Configuration】 Default Configuration is 0, that is, no limit.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】After configuring the limit on the number of new connections for real IPs, some special IPs (such as servers) may need to relax the limit.

【Configuration Example]】Configure the new connection speed of the real IP of the internal network to not exceed 1000, and configure the new connection speed of the server network segment (192.168.1.0/24) to 10000.

```
AC-FS# configure terminal
AC-FS(config)# flow-pre-mgr new-session-limit real-host limit 1000
AC-FS(config)# flow-pre-mgr new-session-limit specify-subnet 192.168.1.0 255.255.255.0 limit 10000
```

【Verification】1. Use show flow-pre-mgr new-session-limit to view the configuration.

2. Use show flow-pre-mgr drop-count to check the packet loss.

3. Use show flow-pre-mgr new-session-limit attack to view the suspected attack source.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.6 flow-pre-mgr new-session-limit { start-up | virtual-host | real-host }

Set the limit on the number of new connections for all virtual IPs within three minutes of device startup, and the flow platform will drop packets if the limit exceeds the limit; Set the limit on the number of newly created virtual IP connections three minutes after the device is turned on, and the flow platform will drop packets if the limit exceeds the limit;
Set the limit on the number of new connections for real IPs, and if the limit is exceeded, the streaming platform will drop packets.

flow-pre-mgr new-session-limit { start-up | virtual-host | real-host } limit limit-number

Remove new connection limit.
no flow-pre-mgr new-session-limit { start-up | virtual-host | real-host }

【Parameter Description】

Parameter	Description
limit-number	Create a new connection limit value in the range of 0-100000.

【Default Configuration】 Default Configuration is 0, that is, no limit

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 In order to prevent the real IP of the intranet from launching a large number of new attacks on the device or the external network due to reasons such as poisoning, you can configure the new connection limit for the intranet IP. Start-up: When the device is just started or the kernel module is reloaded, all online IPs are treated as virtual IPs at the beginning, and the new connection rates of all virtual

IPs are accumulated together for calculation, that is, the new connection limit value It is public. In order to cope with device startup and intranet users going online in a centralized manner, it is necessary to relax the new connection limit at this time (experience value 20000~30000), or set no limit value.

Virtual-host: Three minutes after the device is turned on or the kernel module is reloaded, the new connection rate limit value of the virtual IP, also the new packets of all virtual IPs are accumulated together for the new rate calculation, that is, the new connection limit value is all The virtual IP is public. The experience value is around 3000.

Real-host: The new connection limit of real IP, the new rate of each IP is calculated separately.

【Configuration Example]】 Configure the new connection limit of virtual IP to 20000 within three minutes of device startup; configure the new connection limit of virtual IP to 3000; configure the new connection limit of real IP to 300.

```
AC-FS# configure terminal
AC-FS(config)# flow-pre-mgr new-session-limit start-up limit 20000 AC-
FS(config)# flow-pre-mgr new-session-limit virtual-host limit 3000 AC-
FS(config)# flow-pre-mgr new-session-limit real-host limit 300
```

【Verification】 1. Use show flow-pre-mgr new-session-limit to view the configuration.

2. Use show flow-pre-mgr drop-count to check the packet loss.

3. Use show flow-pre-mgr new-session-limit attack to view the suspected attack source.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

3.7 flow-pre-mgr priority-swap

Switch the priority of two rules

flow-pre-mgr priority-swap rule-id1 rule-id2

【Parameter Description】

Parameter	Description
rule-id1	The rule ID to switch over the priority.
rule-id2	The rule ID to switch over the priority.

【Default Configuration】 None

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Use this command to switch the priority of two rules.

【Configuration Example】Switch the priority of rule 1 and rule 2.

```
AC-FS# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AC-FS(config)# flow-pre-mgr priority-swmp 1 2
```

【Verification】Use show flow-pre-mgr rule-info to view the rule priority after switching. The command priority is ordered from high to low.

【Prompt Information】-

【Common Mistake】 If rule-id1 or rule-id2 does not exist, the command does not perform any processing.

【Platform Description】 -

3.8 flow-pre-mgr protocol-enable

Configuring the Device to Allow OSPF, VRRP, and RIP Protocols.

flow-pre-mgr protocol-enable

Configure no release protocol.

no flow-pre-mgr protocol-enable

【Parameter Description】-

【Default Configuration】 Default release

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Default release.

The processing sequence in the stream pre-creation process is: ip session filte, protocol release, IP new rate limit, buffe protection.

【Configuration Example】Enable protocol release.

```
AC-FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z. AC-
FS(config)# flow-pre-mgr protocol-enable
```

【Verification】Use show flow-pre-mgr protocol-enable to check whether the protocol release is enabled.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.9flow-pre-mgr subscriber

Configure a user/group based session limit value

flow-pre-mgr rule-id subscriber subs_name action {block | by-pass | {trust total-limit total-limit-number per-ip-limit per-limit-number }}

Remove session limit value based on user/user group

no flow-pre-mgr rule-id

【Parameter Description】

Parameter	Description
rule-id	The identification number of the rule, the value range is 1~50. When the configured identification number has been used, a conflict will be displayed and the configuration cannot be successful.
subs_name	The static user or static user group associated with the rule
total-limit-number	The limit value of the total number of streaming sessions of the user/user group, the value is related to the device memory, where 0 means no limit

per-limit-number	The limit value of the number of streaming sessions per IP under the user/user group. The value range is related to the device memory and cannot be greater than total-limit-number, where 0 means no limit.

【Default Configuration】 No related configuration

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 1. Configure the control method of the number of flow sessions based on the user/user group: block, by-pass or trust. To delete the related configuration, execute no flow-pre-mgr id in the global configuration mode. .

2. The configured rules have priority, and the priority is defined according to the principle that the last configured rule has the highest priority.

3. Description of action, block means that flow session communication is not allowed; by-pass means that there is no need to create a flow session, and the message is directly forwarded according to the mapping relationship of the bridge (this command keyword only appears in bridge mode and one-arm mode. , there is no such command keyword in gateway mode); trust indicates that it is allowed to configure the limit of the number of streaming sessions for users/user groups and the number of streaming sessions per IP. After the streaming session exceeds the specified limit value, it is no longer allowed to create new streams. conversational communication.

4. The maximum number of streaming sessions that the device can support is related to the device's memory. When configuring this command, the maximum allowable input is the maximum number of streaming sessions supported by the device.

5. In gateway mode, we do not limit the source-to-source data flow caused by the routing error of the upper-level router.

You must enable Layer 2 and Layer 3 user identification and configure the corresponding user/user group information.

【Configuration Example]】 Configure the user group "UserGroupA" to allow the creation of 5,000 streaming sessions, and each IP under "UserGroupA" is allowed to create 300 streaming sessions, and block the communication of new streams when the limit is exceeded.

```
AC-FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z. AC-
FS(config)# subscriber static name UserGroupA parent /
AC-FS(config)# subscriber static name UserA parent /UserGroupA ip-host 192.168.5.10
AC-FS(config)# subscriber static name UserB parent /UserGroupA ip-host 192.168.5.11 AC-
FS(config)# flow-pre-mgr 1 subscriber UserGroupA action trust total-limit 5000 per-ip-limit 300
```

【Verification】 1. Use show flow-pre-mgr rule-info to view the configured rules and session matching;

2. Use show flow-pre-mgr ip-info to view IP sessions and restrictions.

【Prompt Information】 1: If the rule ID has been used, it will prompt an error.

Rule id already exists, please delete it first

【Common Mistake】 Layer 2 and 3 user identification is not enabled or user/user group information is not configured.

【Platform Description】 -

3.10 flow-pre-mgr total-limit

Configure the total number of sessions limit value.

flow-pre-mgr total-limit limit-number

Remove the total session limit value.

no flow-pre-mgr total-limit

【Parameter Description】

Parameter	Description
limit-number	Global flow session number limit value, the value is related to the device memory size, where 0 indicates no limit.

【Default Configuration】 No related configuration

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 1. The maximum number of streaming sessions that the device can support is related to the device's memory. When configuring this command, the maximum allowed input is the maximum number of streaming sessions supported by the device.

2. In the gateway mode, we do not limit the source-to-source data flow caused by the routing error of the upper-level router.

【Configuration Example】】 Configure a global limit of 200,000 streaming sessions. When the number of streaming sessions reaches 200,000, it is no longer allowed to create streams and will be blocked.

```
AC-FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z. AC-
FS(config)# flow-pre-mgr total-limit 200000
```

【Verification】 1. Use show flow-pre-mgr rule-info to view the configured rules and session matching;

2. Use show flow-pre-mgr ip-info to view IP sessions and restrictions.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.11 flow-pre-mgr upload-pps-limit

Set the upstream packet rate limit of the real IP.

flow-pre-mgr upload-pps-limit limit-number

Delete the upstream packet rate limit.

no flow-pre-mgr upload-pps-limit

【Parameter Description】

Parameter	Description
limit-number	Upper package speed limit value, value range 0-100000.

【Default Configuration】 Default Configuration is 0, that is, no limit.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】This function is usually only enabled when it is necessary to prevent upstream traffic attacks.

This command takes effect for the IPs identified as real IPs, and the upstream packet rate of each real IP is calculated separately.

【Configuration Example]】Configure the real IP upstream packet rate limit to 2000.

```
AC-FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z. AC-
FS(config)# flow-pre-mgr upload-pps-limit 2000
```

【Verification】1. Use show flow-pre-mgr upload-pps-limit to view the configuration;

2. Use show flow-pre-mgr drop-count to check the packet loss status of the upstream packet rate limit.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.12flow-pre-mgr upload-pps-limit { specify | specify-range | specify-subnet }

Set the upstream packet rate limit for the specified IP.

flow-pre-mgr upload-pps-limit { specify ip-addr | specify-range ip-start ip-end | specify-subnet ip-subnet ip-mask } limit limit-number

Delete the upstream packet rate limit of the specified IP.

no flow-pre-mgr upload-pps-limit { specify ip-addr | specify-range ip-start ip-end | specify-subnet

ip-subnet ip-mask }

【Parameter Description】

Parameter	Description
ip-addr	The specific IP as specified.
ip-start	Specifies the start IP for the IP range.
ip-end	Specifies the end IP for the IP range.
ip-subnet	Specifies the subnetwork segment.
ip-mask	Specifies the mask.
limit-number	Upper line package speed limit value, take the value range: 0-100000.

【Default Configuration】 No related configuration

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Usually when the anti-upstream traffic attack is enabled, you can use this command to personalize some special IPs (such as intranet servers).

【Configuration Example]】Configure the number of uplink packets per second for intranet users to not exceed 3,000; 192.168.1.2 This user only allows him to upload a maximum of 10,000 packets per second.

```
AC-FS# configure terminal
AC-FS(config)# flow-pre-mgr upload-pps-limit 3000
```

```
AC-FS(config)# flow-pre-mgr upload-pps-limit specify 192.168.1.2 limit 10000
```

【Verification】1. Use show flow-pre-mgr upload-pps-limit to view the configuration;

2. Use show flow-pre-mgr drop-count to check the packet loss status of the upstream packet rate limit.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

3.13 ip session filter

Configure New Stream Filtering.

Ip session filter acl-id

Delete new stream filter.

no ip session filter

【Parameter Description】

Parameter	Description
acl-id	The ID number of the ACL, used for new message filtering.

【Default Configuration】 No related configuration

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】Before the device establishes a flow, perform ACL filtering to allow only the packets of legitimate IP addresses to establish the flow, and block the others.

【Configuration Example]】The configuration allows only the IP of the 192.168.1.0 network segment to establish traffic, and all others are blocked.

```
AC-FS# configure terminal
Enter configuration commands, one per line. End with CNTL/Z. AC-
FS(config)# ip access-list extended 190
AC-FS(config-ext-nacl)# 10 permit ip 192.168.1.0 0.0.0.255 any
AC-FS(config-ext-nacl)# exit
AC-FS(config)# ip session filter 190
```

【Verification】 1. Use show flow-pre-mgr drop-count to check the number of packets filtered by ACL.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

3.14 show flow-pre-mgr drop-count

View buffer-protected logging.

show flow-pre-mgr drop-count

【Parameter Description】 -

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】 14

【Usage Guide】 Use this command to check the number of lost packets of each sub-function.

【Configuration Example】 View the number of lost packets.

```
AC-FS#show flow-pre-mgr drop-count
DROP-TYPE            DROP-PKT
================================
Filter-pkt                      42892 Session-
real                         0  Session-specify
0  Session-virtual                          970
Session-cpu                               0 PPS-
real                              0 PPS-specify
0 PPS-virtual                             0 Buff-
real  0
Buff-virtual         0
```

【Prompt Information】-

【Platform Description】 -

3.15 show flow-pre-mgr ip-info

View IP sessions and limit Parameter.

show flow-pre-mgr ip-info [ip-address]

【Parameter Description】

Parameter	Description
ip-address	View the session of the specified IP and limit the Parameter.
default	If the ip-address Parameter is not specified, view all of the IP.

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】 14

【Usage Guide】 Use this command to view the number of IP sessions and limit Parameter

【Configuration Example】View IP sessions and limit Parameter

```
AC-FS#show  ip  pim  sparse-mode  interface  detail  AC-FS#show
flow-pre-mgr ip-info
IP-ADDRESS                    flow-cnt    flow-limit
```

```
==================================================


192.168.10.1                                500
203
192.168.10.2                                500
103
192.168.10.3                                0
20
192.168.10.4                                0
15
AC-FS#
```

Field Description:

field	Description
IP-ADDRESS	IP address.
flow-cnt	Current session count.
flow-limit	Session limit value.

【Prompt Information】-

【Platform Description】 -

3.16 show flow-pre-mgr new-session-limit

View the configured anti-new attack rules.

show flow-pre-mgr new-session-limit

【Parameter Description】-

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】 14

【Usage Guide】 Use this command to view the new connection limit configuration of the current device.

【Configuration Example】View configuration.

```
AC-FS# show flow-pre-mgr new-session-limit
flow-pre-mgr new-session-limit start-up limit 20000
flow-pre-mgr new-session-limit virtual-host limit 10000
flow-pre-mgr new-session-limit real-host limit 1000
flow-pre-mgr new-session-limit specify-host 192.168.1.110 limit 5000
flow-pre-mgr new-session-limit specify-host 192.168.1.112 limit 10000
```

【Prompt Information】-

【Platform Description】 -

3.17 show flow-pre-mgr new-session-limit attack

View log records for the last newly created attack.

show flow-pre-mgr new-session-limit attack

【Parameter Description】-

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】 14

【Usage Guide】 Use this command to view the record of the latest new connection attack on the current device.

【Configuration Example】View configuration.

```
AC-FS# show flow-pre-mgr new-session-limit attack
HOST-TYPE           HOST-IP             TIME

============================================================
real-host.....172.18.8.156         2014-10-16 14:15:28
```

【Prompt Information】-

【Platform Description】 -

3.18 show flow-pre-mgr rule-info

View configured rules.

show flow-pre-mgr rule-info

【Parameter Description】-

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】 14

【Usage Guide】 Use this command to view the configured rules and session matching.

【Configuration Example]】View the configured rules and session matching.

```
AC-FS#show flow-pre-mgr rule-info
flow-pre-mgr total-limit 200000
(active)flow-pre-mgr 1 subscriber UserGroupA action trust total-limit 5000 per-ip-limit 300 (446
flows)
(inactive)flow-pre-mgr 2 access-list 120 action block (0 flows)
```

Field Description:

field	Explain
active	The rule is currently in effect status.
inactive	The rule is currently not in effect status.
flows	How many sessions currently match this rule.

【Prompt Information】-

【Platform Description】 -

3.19 show flow-pre-mgr upload-pps-limit

View the configured anti-upstream traffic attack rules.

show flow-pre-mgr upload-pps-limit

【Parameter Description】-

【Command Mode】 Privileged mode, global mode, interface mode

【Default Level】 14

【Usage Guide】 Use this command to view the configuration of upstream packet rate limit per IP.

【Configuration Example】 View configuration.

```
AC-FS# show flow-pre-mgr upload-pps-limit
flow-pre-mgr upload-pps-limit 3000
flow-pre-mgr upload-pps-limit specify 192.168.1.30 limit 5000
flow-pre-mgr upload-pps-limit specify 192.168.1.20 limit 10000
```

【Prompt Information】 -

【Platform Description】 -

4 FLOW-CONTROL

4.1active-limit

Enable precise P2P rate limiting (for TCP or UDP).

active-limit { tcp-enable | udp-enable }

Turn off precise P2P rate limiting.

no active -limit { tcp-enable | udp-enable }

【Parameter Description】

Parameter	Description
tcp-enable	TCP exact speed limit switch.
udp-enable	UDP exact speed limit switch.

【Default Configuration】 Open by default

【Command Mode】 flow-control configuration mode

【Default Level】 14

【Usage Guide】 1. Predict the downlink congestion in advance, and notify the peer to slow down the sending rate by affecting the uplink traffic. It is an end-to-end speed limiting method, mainly used for speed limiting of P2p applications;

2. In order to avoid affecting key applications such as video and voice, the active speed limit only takes effect for channels with a priority value greater than or equal to 4 (the higher the value, the lower the priority).

【Configuration Example]】 1: Disable the UDP active rate limit function of the policy group group1:

```
AC-FS# config
AC-FS(config)# flow-control group1
AC-FS(config-flow-control)# no active-limit udp-enable
```

【Verification】 1: Use show flow-control {NAME} to view the configuration of the entire flow control group. If the following display is displayed, it means that P2P precise rate limiting (UDP or TCP) is enabled:

```
no active-limit tcp-enable
no active-limit udp-enable
```

【Prompt Information】 -

【Common Mistake】-

【Platform Description】 -

4.2auto-pir

Enables the PIR dynamic adjustment function of the flow control channel tree.

auto-pir enable [interval NUM [root-rate Percentage]] [exclude-pass]

Disable the PIR dynamic adjustment function for the number of flow control channels.

no auto-pir enable

【Parameter Description】

Parameter	Description
NUM	Adjust interval in seconds, default 1 second and configuration range 1 to 3600
Percentage	PIR suppression or recovery valve value: root channel bandwidth utilization, the processing logic is as follows： The PIR suppression check is triggered above the threshold, following the channel priority and suppressing the PIR if the channel rate exceeds the CIR； PIR recovery is triggered 10% below threshold from high to low per channel priority； Do not process when in between No configuration default is 90, configuration range of 1 to 99...With the default value of 90, PIR recovery is triggered below 80%, PIR suppression check is triggered above 90%, and no processing is done when being between 80% and 90%.
exclude-pass	After the keyword "exclude root" is entered, the default value is not included Pass traffic.

【Default Configuration】 EG products are enabled by default, and NPE products are disabled by default.

【Command Mode】 channel-tree configuration mode.

【Default Level】 14

【Usage Guide】Applicable to the scenario where the upper-level flow control device exists. If the bandwidth occupied by point-to-point traffic remains high and the bandwidth of other applications cannot be guaranteed, this function can be enabled.

The root bandwidth utilization calculated here is the actual utilization, including traffic forwarded and discarded by flow control.

【Configuration Example]】Enable the PIR adjustment function of the inbound channel tree of the policy group group1:

```
AC-FS(config)# config AC-FS(config)#
flow-control group1
AC-FS(config-flow-control)# channel-tree inbound
AC-FS(config-channel-tree)# auto-pir enable
```

【Verification】Use show flow-control Name [inbound | outbound] auto-pir to check whether auto-pir takes effect.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

4.3 change-priority

Swap the priorities of two policy rules under the same flow control group:

change-priority rule1 rule1-num rule2 rule2-num [by-rule-number]

【Parameter Description】

Parameter	Description
rule1-num	Exchange the number of the first policy rule, the default priority number.
rule2-num	Exchange the number of the second policy rule, the default priority number.
by-rule-number	Input indicate that rule1-num and rule2-num are rule Number instead of the default prioritization number.

【Default Configuration】 None

【Command Mode】 Flow control group configuration mode

【Default Level】 14

【Usage Guide】The priority number of the policy rule can be viewed through Pri_num Field in show flow-control-policy rule [group name].

【Configuration Example]】1: Exchange the priorities of two policy rules with priority numbers 1 and 2 under the flow control group

group1. Note that 1 and 2 are priority numbers:

```
AC-FS(config)# config AC-FS(config)#
flow-control group1
AC-FS(config-flow-control)# change-priority rule1 1 rule2 2
```

【Verification】Use the show flow-control-policy rule [group name] command to view the detailed information of all policy rules or policy rules under a specific flow control group.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

4.4channel-default

Specifies the default flow control channel.

channel-default channel-name

Restore Default Configuration.

no channel-default

【Parameter Description】

Parameter	Description
channel-name	The flow control channel name has been configured.

【Default Configuration】 By default, it is the root channel.

【Command Mode】 channel-tree configuration mode

【Default Level】 14

【Usage Guide】 By configuring this command, all traffic that fails to match the flow control policy will enter the specified default channel

【Configuration Example】】Specify the channel "depart5" in the downstream flow control tree of the flow control group "test" as the default channel.

```
AC-FS(config)#flow-control test
AC-FS(config-flow-control)#channel-tree inbound AC-
FS(config-channel-tree)#channel-default depart5
```

【Verification】Use show flow-control {NAME} to view the configuration of the entire flow control group.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

4.5channel-group

Create a flow control channel.

channel-group name parent { NULL | parent_name } [cir cir_num] [pir pir_num] [pri pri_num] { fifo |

{ per-net [per-mask mask] | per-user } per-pir ppir_num [limit limit_num] [session-limit

session_limit_num] [reverse] }

Configure the flow control channel to join the shared pool.

channel-group name pool pool_name

Delete flow control channel.

no channel-group name

Delete the flow control channel shared pool.

no channel-group name pool pool_name

【Parameter Description】

Parameter	Description
name	Create the name of the channel
parent	Create the parent channel for the channel
NULL	If no parent channel exists, the channel is created as the root channel of the flow control tree
parent_name	The parent channel name that creates the channel and must be the channel already created
cir cir_num	Acknowledge information rate, the minimum bandwidth guaranteed, input range of 100 to 10000000, in kbps, no input default 0, no bandwidth shortage, the root node is not allowed to be configured to 0.

pir pir_num	The peak information rate, that is, the maximum bandwidth, must be greater than or equal to cir, the part beyond cir is the bandwidth borrowed from the parent channel, the input range is 100 to 10000000 in kbps PIR does not enter the default parent PIR, if the parent does not exist, take the value of CIR.
pri pri_num	Priority, input range 0~7,0 highest priority, high priority channels are preferentially scheduling
fifo	First in first out queue.
per-net	Fair queues per network segment, the number of internal queues is not fixed, based on the network segment to achieve a fair opportunity to send packets, suitable for congested channels, it also needs to configure the following Parameter.
per-mask mask	Network segment mask, the input range is 1～32, when 32 is based on each IP fairness, if not input, the default is 32.
per-user	Fair queue per account, the number of internal queues is not fixed, based on each account to achieve a fair opportunity to send packets, suitable for congested channels.
per-pir ppir_num	Peak information rate for each network segment, maximum bandwidth, input range of 1 ~ 10000000 in kbps.
limit limit_num	Limit the number of network segments, the input range is 1～65535, if not input, the default value will be taken according to the total bandwidth size, if the total bandwidth is less than 100M, take 1000, if the total bandwidth is greater than or equal to 100M, take 10000.
session-limit session_limit_num	Used to limit the number of connections per network segment (IP), the input range is 1 to 65535, the default is not to limit the number of connections per IP.
pool pool_name	Configure the name of the flow control channel added to the shared pool, which is not supported by NPE products.
reverse	(Optional) Reverse Per-net, speed limit for external network segment (IP), speed limit for access branch public network segment (IP) in VPN scenario, default is forward Per-net.

【Default Configuration】 By default, no flow control channel is configured.

【Command Mode】 channel-tree configuration mode

【Default Level】 14

【Usage Guide】 1. There can only be one root channel in a flow control tree, and the cir and pir of the root channel need to be set to the same value;

2. When the channel cir is configured, it is required that the sum of the configured cir and all its sibling channel cirs is less than or equal to the parent channel's cir; when the channel's pir is configured, it is required that the configured pir must be less than or equal to the parent

channel's pir;

3. High-priority channels are scheduled first, and the probability of packet loss is lower in the case of congestion;

4. The per-net queue and the per-user queue are fair queues. Only in the case of congestion, the configuration is meaningful, and it will reflect the characteristics of fair packet distribution;

5. The network segment traffic beyond the per-net queue limit will enter the default queue of the per-net queue. The default queue has the lowest packet priority, and the bandwidth of the network segment within the limit will be guaranteed first. In addition, per-pir, limit and session-limit do not support nesting. For example, the root channel limit session-limit is 1000, the root channel sub-channel limit BT session-limit is 500, the actual meaning is non-BT traffic limit session- The limit is 1000, and the BT limit is 500;

6. Only the bottom two layers of the flow control tree are supported to join the shared pool, that is, only leaf channels and their parent channels are allowed to join the shared pool, and the shared pool must have been created;

7. To join the Per-IP type shared pool, the channel type must be Per-IP type, that is, Per-net and per-mask is 32, and the limit cannot be greater than the limit of the shared pool;

8. The number of shared pool member channels cannot exceed 8;

9. The channel of per-user type does not support joining the shared pool.

【Configuration Example]】 Create a channel named "root" on the downstream flow control tree of the flow control group "test":

```
AC-FS(config)#flow-control test
AC-FS(config-flow-control)#channel-tree inbound
AC-FS(config-channel-tree)#channel-group root parent null cir 50000 pir 50000 pri 4 fifo
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

4.6channel-tree

Create a flow control channel tree.

channel-tree { inbound | outbound }

Remove the number of flow control channels.

[no] channel-tree { inbound | outbound }

【Parameter Description】

Parameter	Description
inbound	go down.
outbound	Up going.

【Default Configuration】 The flow control tree is not configured by default.

【Command Mode】 Flow-control mode

【Default Level】 14

【Usage Guide】A flow control group should include a flow control tree in the downstream direction and a flow control tree in the upstream direction.

【Configuration Example]】Create a downstream flow control tree and an upstream flow control tree in the flow control group "test":

```
AC-FS(config)#flow-control test
AC-FS(config-flow-control)#channel-tree inbound
AC-FS(config-channel-tree)#exit
AC-FS(config-flow-control)#channel-tree outbound
AC-FS(config-channel-tree)#exit
```

【Verification】Use show flow-control { NAME } to view the configuration of the entire flow control group.

【Prompt Information】 None

【Common Mistake】 None

【Platform Description】 -

4.7 clear flow-control

Configure the Description of the flow control group.

clear flow-control name statistics

【Parameter Description】

Parameter	Description
name	Stream control group name, supported by up to 32 characters.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Clear the flow control group data statistics value.

【Configuration Example]】To clear the statistics of the flow control group "Gi0/1":

```
AC-FS# clear flow-control Gi0/1 statistics
```

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

4.8comment

Configure the Description of the flow control group.

comment Comment_String

Delete an already configured description field.

[no] comment Comment_String

【Parameter Description】

Parameter	Description
Comment_String	Description string, with maximum support of 127 characters, and no spaces in the middle.

【Default Configuration】 Description field is not configured by default.

【Command Mode】 flow-control configuration mode

【Default Level】 14

【Usage Guide】 None

【Configuration Example]】Configure the DescriptionField in the flow control group "Gi0/1":

```
AC-FS(config)#flow-control Gi0/1
AC-FS(config-flow-control)# comment Dianxin-10M
```

【Verification】Use show flow-control {NAME} to view the configuration of the entire flow control group.

【Prompt Information】 None

【Common Mistake】 None

【Platform Description】 -

4.9flow-control

Configure a flow control group (referred to as a flow control group).

flow-control { statistics | log on | name [update bandwith In_bandwith Out_bandwith [perpir-update]] }

Delete a specific flow control group.

no flow-control name

【Parameter Description】

Parameter	Description
statistics	Flow control forward message data information statistical switch (except high performance equipment, open statistical switch by default).
log	Flow-control Log switch.
on	Log switch.
name	The name of the traffic control group.
In_bandwith	Expected updated downlink bandwidth size, input range: 500 to 10000000, in kbps.
Out_bandwith	Upink bandwidth size expected to update, input range: 500 to 10000000 in kbps.
perpir-update	If input, Per-PIR will always be adjusted proportionally with the bandwidth. Without input, when the bandwidth is greater than the reference bandwidth by 10M, the proportional adjustment will be made.

【Default Configuration】 By default, only the flow control template configuration exists in the system.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 1. Enter the flow control group mode by configuring this command. Based on this flow control group, you can further configure the flow control policy rules and flow control channels. It should be noted that the flow control group must be applied to the WAN port for the policy rules and channels to take effect.

2. Use the update keyword to update the bandwidth of the existing flow control group. Among them, the bandwidth update affects all shared pool and channel bandwidth configurations, and will be adjusted proportionally.

【Configuration Example】1: Configure flow control policy group group 1.

```
AC-FS#config
AC-FS(config)#flow-control group1
```

2: Configure flow control policy group group2.

```
AC-FS#config
AC-FS(config)#flow-control group1
```

3: Delete the flow control policy group group1.

```
AC-FS#config
AC-FS(config)#no flow-control group1
```

4: Update the bandwidth size of Gi0/0 to 20M.

```
AC-FS#config
AC-FS(config)#flow-control Gi0/0 update bandwith 20000 20000
```

【Verification】Use show flow-control {NAME} to view the configuration of the entire flow control group.

【Prompt Information】 None

【Common Mistake】 None

【Platform Description】 -

4.10flow-policy

Apply the flow control group to the wan port, so that the flow control policy rules and flow control policy channels configured under this policy group can take effect:

flow-policy name

To cancel the application of a specific flow control group on an interface:

no flow-policy

【Parameter Description】

Parameter	Description
name	The name of the traffic control group.

【Default Configuration】 By default, no flow control group is applied to the WAN port in the system.

【Command Mode】 Interface configuration mode

【Default Level】 14

【Usage Guide】 This command can only be configured on the WAN port, and cannot be used on the non-WAN port.

【Configuration Example]】1: The flow control policy group group1 is applied to interface gi0/1:

```
AC-FS#config AC-FS(config)#interface
gi0/1
AC-FS(config-if-GigabitEthernet 0/1)#flow-policy group1
```

2: Cancel the application of flow control policy group group1 on interface gi0/1:

```
AC-FS#config AC-FS(config)#interface
gi0/1
AC-FS(config-if-GigabitEthernet 0/1)#no flow-policy
```

【Verification】Run the show run command to check whether flow control is configured on the interface.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

4.11 flow-rule

To configure a flow control policy rule, it needs to be configured in two parts. The first part represents the keyword of the policy rule, and the second part represents the action of the policy rule:

flow-rule num [vlan-group vlan-group-name] [subscriber subscriber-name] [auth-group auth-group-name] [network-group network-group-name] [app-group app-group-name] time-range time-range-name [vpn]

flow-rule num action { drop | log-drop | pass [in-channel in-channel-name] [out-channel

out-channel-name] } [default] [commet string]

Delete a policy.

no flow-rule num

A policy is prohibited.

flow-rule num disable

Policy unblocks.

no flow-rule num disable

【Parameter Description】

Parameter	Description
num	Number of the flow control policy rule, enter range 1 to 8192.
vlan-group-name	Name of the vlan-group object associated with the policy rule, any means that matches any object.
subscriber-name	The name of the subscriber object associated with the policy rule, any means matching any object.
auth-group-name	The authentication object name associated with the policy rule, any means matching any authentication object.
network-group-name	The name of the network-group object associated with the policy rule, any means matching any object.
app-group-name	The name of the app-group object associated with the policy rule, and any means matching any object.

time-rang-name	The name of the time-rang object associated with the policy rule.
in-channel-name	The name of the in-channel channel associated with the policy rule.
out-channel-name	Name of the out-channel channel associated with the policy rule.
string	Comments to the policy rule..
disable	Disable the policy rule, and the default is non-disabled
vpn	Configure VPN policy, only match VPDN traffic, the default is non-VPN policy
default	Default policy, the lowest priority, default policies based on the thinner the more priority principle.

【Default Configuration】 By default, no policy rules are configured in the system.

【Command Mode】 Flow control group configuration mode

【Default Level】 14

【Usage Guide】 1. It is not allowed to configure policy rules with different num numbers but the same keywords.

2. The principle of policy rule matching is that the configuration will take effect first. The conditions for the policy rule to take effect require that both parts of the policy have been configured, the associated objects and channel objects have been configured, and the traffic control group where the policy rule is located has been applied to WAN port.

3. When the policy configuration Action is pass, if the in-channel or out-channel is not configured, the corresponding in or out direction will not limit the speed, and if neither direction is configured, it means that there will be no speed limit in both directions;

4. The policy refinement judgment principle: first compare the object priority, vlan object > intranet IP object > authentication object > external network IP object > application identification object; when the object priority is the same, the comparison basis of the same object is that the subclass is compared to the parent The class is more refined. For example, Aliwangwang belongs to instant messaging software, and other objects are the same. Compared with the application object's strategy of using instant messaging software, the strategy of using Aliwangwang is more refined.

【Configuration Example]】 1: Under the flow control group group1, configure the egress bandwidth limit of a company's administrative department to 3M.

```
AC-FS#config
AC-FS(config)#flow-control group1
AC-FS(config-flow-control)#flow-rule 1 vlan-group any subscriber Administration Department network-group any app-group any time-rang any
AC-FS(config-flow-control)#flow-rule 1 action pass out-channel Export bandwidth of administration department 3M
```

2: Under the flow control group group2, configure the restriction that Zhang San of the administrative department of a company is not

allowed to access sina during working hours.

```
AC-FS#config
AC-FS(config)#flow-control group1
AC-FS(config-flow-control)#flow-rule 1 vlan-group any subscriber  network-group sina app-group any time-rang work
AC-FS(config-flow-control)#flow-rule 1 action drop
```

【Verification】 -

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

4.12flow-template

Take an existing flow control group as a template, copy a new configuration, and update the bandwidth size, which is used to quickly generate a new configuration based on the template or other flow control groups during the deployment phase:

flow-template copy Src_name Dst_name [bandwith In_bandwith Out_bandwith [perpir-update]] [force]

【Parameter Description】

Parameter	Description
Src_name	The source flow control group of the copy, that is, the flow control group name used as the template.
Dst_name	The name of the newly created flow control group, which is not allowed to be the same as Src_name.
In_bandwith	Expected downlink bandwidth size to be updated, input range: 500~ 10000000, unit: kbps, do not enter the downlink bandwidth size of the default source configuration group.
Out_bandwith	Expected upstream bandwidth size to be updated, input range: 500~ 10000000, unit: kbps, do not enter the upstream bandwidth size of the default source configuration group.
perpir-update	If it is input, Per-PIR will always be adjusted proportionally with the bandwidth, and when the bandwidth is not input, when the bandwidth is greater than the reference bandwidth by 10M, it will be adjusted in proportion.

force	If the target flow control group already exists, if force is not entered, the copy will fail, and if force is entered, the existing flow control group will be deleted before starting the copy.

【Default Configuration】-

【Command Mode】 Global mode

【Default Level】 14

【 Usage Guide 】 1. The bandwidth update affects all shared pool and channel bandwidth configurations, and will be adjusted proportionally.

2. The configuration copy is used to generate a new configuration according to the existing flow control group configuration template, and the bandwidth update therein can be considered as performing bandwidth update for the newly created flow control group.

【Configuration Example】Generate a new flow control group BBB according to the flow control group AAA, and update the bandwidth to 15M.

```
AC-FS#config
AC-FS(config)# flow-template copy AAA BBB bandwith 15000 15000
```

【Verification】-

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

4.13 share-pool

Create a shared pool.

share-pool Name rate num1 [type { normal | per-ip [limit num2l }]

Delete the shared pool.

no share-pool Name

【Parameter Description】

Parameter	Description
Name	Shared pool name.
num1	Create a shared pool bandwidth.
type	Create a shared pool type, without entering the default to the normal type.
normal	normal type, speed limit for total bandwidth for all users.
per-ip	Type per-ip, speed limit per user bandwidth.
num2	Limit of users for per-ip type shared pool.

【Default Configuration】 By default, no shared pool is configured in the system.

【Command Mode】 channel-tree configuration mode

【Default Level】 14

【Usage Guide】 1. The Normal type shared pool limits the bandwidth based on all users who join the shared pool channel, that is, the bandwidth of all users cannot exceed the configured Rate; 2. The Per-IP type shared pool limits the bandwidth based on each user who joins the shared pool channel, that is, the bandwidth of each user cannot exceed the configured Rate.

3. If the user exceeds the limit of the Per-IP type shared pool limit, the traffic will be cut off. Limit will automatically generate a Limit value without input;

4. Channels that join the shared pool have different priorities. In the worst case, the channel with high priority will occupy all the bandwidth of the shared pool, which can be used in scenarios where different services need to be prioritized.

【Configuration Example]】In the inbound flow control tree of the flow control group group1, create a shared pool test of type Normal and bandwidth of 1000kbps:

```
AC-FS#config
AC-FS(config)#flow-control group1
AC-FS(config-flow-control)# channel-tree inbound
AC-FS(config-channel-tree)# share-pool test rate 1000 type normal
```

【Verification】Use show flow-control { NAME } to view the configuration of the entire flow control group.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

4.14 show flow control

Display flow control group configuration information. If no flow control group is specified, all flow control group configurations will be displayed:

show flow-control [Name]

Display the configuration information of the flow control channel:

show flow-control Name { inbound | outbound } [channel-group channel-name [detail]]

Display shared pool configuration information (not supported by NPE products):

show flow-control Name { inbound | outbound } [share-pool [pool-name]]

Display auto-pir status information:

show flow-control Name [inbound | outbound] auto-pir

【Parameter Description】

Parameter	Description
Name	The name of the flow control group.
inbound	Downstream flow control tree.
outbound	Upstream flow control tree.
channel-name	Configuration of the flow control channel, plus the detail keyword to display FIFO, SFQ and Per-net.
pool-name	Queue running status information.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 If you enter the channel-group channel-name keyword, only the configuration information of the corresponding channel will be displayed, otherwise, the configuration information of all channels configured on the entire flow control channel tree will be displayed.

【Configuration Example】1 Display the configuration information of the specified flow control group: Gi0/6.

```
AC-FS#sh flow-control test flow-control test
 comment tpl-ibar
 !
 channel-tree inbound
  auto-pir enable interval 1 root-rate 90
  !
  channel-group root parent null cir 130000 pir 130000 pri 4 per-net per-mask 32 per-cir 130 per-pir 2000 limit 1000
  channel-group key parent root cir 65000 pir 91000 pri 0 per-net per-mask 32 per-cir 65 per-pir 78000 limit 1000
  channel-group normal parent root cir 52000 pir 91000 pri 4 per-net per-mask 32 per-cir 52 per-pir 78000 limit 1000
  channel-group unkey parent root cir 13000 pir 52000 pri 7 per-net per-mask 32 per-cir 13 per-pir 3003 limit 1000
  channel-default normal
 !
 channel-tree outbound
  no auto-pir enable
  !
  channel-group root parent null cir 130000 pir 130000 pri 4 per-net per-mask 32 per-cir 130 per-pir 2000 limit 1000
  channel-group key parent root cir 65000 pir 78000 pri 0 per-net per-mask 32 per-cir 65 per-pir 4998 limit 1000
  channel-group normal parent root cir 52000 pir 78000 pri 4 per-net per-mask 32 per-cir 52 per-pir 3003 limit 1000
  channel-group unkey parent root cir 13000 pir 52000 pri 7 per-net per-mask 32 per-cir 13 per-pir 3003 limit 1000
  channel-default normal
 !
 flow-rule 1000 app-group Other_Group time-range any
 flow-rule 1000 action pass in-channel normal out-channel normal default comment
Match_Normal_Group_of_NON_VPN
 flow-rule 999 app-group Key_Group time-range any
 flow-rule 999 action pass in-channel key out-channel key default comment Match_Key_Group_of_NON_VPN
 flow-rule 998 app-group Unkey_Group time-range any
 flow-rule 998 action pass in-channel unkey out-channel unkey default comment Match_Inhib_Group_of_NON_VPN
 flow-rule 992 subscriber VIP time-range any
 flow-rule 992 action pass in-channel key out-channel key comment Match_VIP_Group_of_NON_VPN
flow-rule 991 network-group Out_Server time-range any
```

```
flow-rule 991 action pass in-channel key out-channel key comment Match_Out_Server_of_NON_VPN
flow-rule 900 app-group TC_AD_Key time-range any
flow-rule 900 action pass in-channel key out-channel key comment Match_AD_Key_of_NON_VPN
flow-rule 900 disable
```

2 Display the configuration information of the specified channel in the downstream direction:

```
AC-FS#sh flow-control test inbound channel-group root
Group-name                          CIR      PIR      Pri  Schedule
CIDR/CIR/PIR/Limit/Sess-limit/Share-pool  R
------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------
root                                130000      130000      4       per-net     32/130/2000/1000/0
0
```

3 Display the configuration information of all channels downstream of the channel tree:

```
AC-FS#sh flow-control test inbound
Group-name                          CIR      PIR      Pri  Schedule
CIDR/CIR/PIR/Limit/Sess-limit/Share-pool  R
------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------
root                                130000      130000      4       per-net     32/130/2000/1000/0/
0
key                                 65000       91000       0       per-net     32/65/78000/1000/0/
0
normal                              52000       91000       4       per-net     32/52/78000/1000/0/
0
unkey                               13000    52000    7    per-net  32/13/3003/1000/0/
0
```

Field Description:

Field	Description
Group-name	The channel name.
CIR	committed information rate, CIR.
PIR	Peak information rate.
Pri	Channel priority.
Schedule	Channel queue type.
CIDR/CIR/PIR/Limit/Sess-limit/Share-pool	CIDR/CIR/PIR/Limit/Sess-limit/Share-pool.

4 Display the configuration information of all upstream shared pools:

```
AC-FS#show flow-control test outbound share-pool
Global pool:     14           Global   red   obj:    0
Tree pool:       3
```

```
Share-pool      Rate        Type        Limit       Child
_____________ __________ __________ __________ __________

tcp                 200           Normal        NA             1
udp                 150           Normal        NA             1
p1  100  Normal  NA  2
```

Field Description:

Field	Description
Global pool	Number of global shared pools.
Global red obj	The limit shared pool object is reached globally, and statistics are made for each node of the Normal type shared pool and the Per-IP type shared pool.
Tree pool	The number of shared pools corresponding to Channel-tree.
Share-pool	Shared pool name.
Rate	Shared pool rate limit.
Type	Shared pool type.
Limit	Per-IP type shared pool is valid, and the number of users is limited.
Child	The number of member channels. Note that only the number of channels added to the pool is calculated. If the parent channel of three leaves is added to the shared pool, the statistic value is only added by 1.

5 Display the information of the upstream specified shared pool:

```
AC-FS#show flow-control test3 outbound share-pool p1
Pool: p1
Rate:        100         Type:        Normal       Limit:       NA
State:       Green       Child:       2            Active:      NA
Kill flow: 0

Group-name  Cir     Pir      Pri  Type       Limit     Share-pool
___________ _____ _______ ____ ________ ________ __________

p1-tcp      150      500      4    fifo       NA            p1 p1-
udp      100      500      4    fifo       NA  p1
```

Field Description:

Field	Description
Pool	Shared pool name.
Rate	Shared pool rate limit.
Type	Shared pool type.

Limit	Per-IP type shared pools are valid and limit the number of users.
State	The Normal type shared pool is valid, Green indicates that the limit value has not been reached, Red indicates that the upper limit value has been reached, and the Per-IP type is the number of NA member channels. Note that only the number of channels added to the Pool is calculated. If the parent channel of three leaves is added to the shared pool, the The statistic is only incremented by 1.
Child	Per-IP type shared pools are valid and limit the number of users.
Limit	Number of active users, valid for Per-IP type shared pools.
Active	Statistics on the number of end flows, the Per-IP type shared pool is valid, and the count of the end times of user traffic exceeding the Limit limit of the Per-IP type shared pool is counted.
Kill flow	Shared pool type..
Group-name	Shared pool member channel name.
Cir	Shared Pool Member Channel Commitment Bandwidth.
Pir	Shared Pool Member Channel Peak Bandwidth.
Type	Shared Pool Member Channel Type.
Pri	Shared Pool Member Channel Priority.
Limit	Shared pool member channel user limit, valid for Per-net type.
Share-pool	The channel joins the shared pool name. Note: If it is specified that the existing members of the shared pool are non-leaf channels, the sub-channels of the non-leaf channel will also be displayed through this command. If the sub-channels have joined another shared pool, the Share-pool will display the corresponding name, otherwise it will be NA.

【Prompt Information】-

【Platform Description】 -

4.15 show flow-control-policy group

Displays details of flow control groups.

show flow-control-policy group

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Displays the detailed information of all flow control groups in the system, including the name of the flow control group, the number of the flow control group, the index value of the interface to which the flow control group is applied, and the overall policy rules configured under the flow control group. number.

【Configuration Example】Display the detailed information of all flow control groups in the system:

```
AC-FS#show flow-control-policy group
group_name                      group_id  apply_ifx     policy_entries

group1                           0          6              14
group2                           1          0              4
```

Field Description:

Field	Description
group-name	The name of the traffic control group.
group-id	Number of the flow control group.
apply_ifx	The interface index value of the flow control group application, 0 means it is not applied to any interface.
policy_entries	The number of flow control policy rule bars configured under this flow control group.

【Prompt Information】-

【Platform Description】 -

4.16 show flow-control-policy rule

Displays the detailed information of flow control policy rules.

show flow-control-policy rule [group name]

【Parameter Description】

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】The use case displays the detailed information of all policy rules in the system or policy rules under a certain traffic control group, including the number, priority number of each policy rule, the index value of the interface to which the policy rule belongs, the id of each object, How many flows currently match this policy rule, the maximum number of sessions for this policy rule, and the validity of the policy rule.

【Configuration Example】 Display the detailed information of all flow control groups in the system:

```
AC-FS#sh flow-control-policy rule
Some comment:
| prio   : priority of the rule | grp      : group the rule located | rule : rule number in group |
| ifx  : interface correspond | vlan_id : vlan identify     | subs_id : subscriber identify
|
| auth_id : auth_group identify | net_wk_id : network identify     | app_id : application
```

```
 identify |
 | in     : in-channel identify | out     : out-channel identify | ses_now : session hold now
 |
 | ses  : config session     | stat    : disable or enable     | ef    : the effect of the rule |

 prio grp rule ifx vlan_id    subs_id    auth_id    net_wk_id app_id    in   out   ses_now ses stat ef
 73   5 1000 0   4294967295 4294967295 4294967295 4294967295 4294967288 5    5    0     0 up 0
 74   5   999   0    4294967295 4294967295 4294967295 4294967295 4294967290 1    1    0      0 up 0
 75   5 998 0   4294967295 4294967295 4294967295 4294967295 4294967289 6    6    0     0 up 0
 76   5 997 0   4294967295 4294967295 4294967295 4294967295 4294967295 4    4    0     0 up 0
 77  5 996 0  4294967295 4294967295 4294967295 4294967295 0         3  3    0  0 up 0
 78  5 995 0  4294967295 4294967295 4294967295 4294967295 0         2  2    0  0 up 0
 79  5 994 0  4294967295 20069752 4294967295 4294967295 4294967295 2     2    0     0 up 0
 80  5 993 0  4294967295 4294967295 4294967295 19787672   4294967295 2     2    0  0 up 0
 81  5 992 0  4294967295 20069752 4294967295 4294967295 4294967295 1     1    0     0 up 0
 82  5 991 0  4294967295 4294967295 4294967295 19787672   4294967295 1     1    0  0 up 0
 83   5 900 0   4294967295 4294967295 4294967295 4294967295 4144963584 1    1    0     0 down 0
 84   6 1000 0   4294967295 4294967295 4294967295 4294967295 4294967288 5    5    0     0 up 0
 85   6 999 0   4294967295 4294967295 4294967295 4294967295 4294967290 1    1    0     0 up 0
 86   6 998 0   4294967295 4294967295 4294967295 4294967295 4294967289 6    6    0     0 up 0
 87   6 997 0   4294967295 4294967295 4294967295 4294967295 4294967295 4    4    0     0 up 0
 88  6 996 0  4294967295 4294967295 4294967295 4294967295 0         3  3    0  0 up 0
 89  6 995 0  4294967295 4294967295 4294967295 4294967295 0        2  2    0   0
```

```
up  0
90  6 994 0  4294967295 20069752 4294967295 4294967295 4294967295 2   2   0    0 up 0
91  6 993 0  4294967295 4294967295 4294967295 19787672 4294967295 2   2   0    0 up 0
92  6 992 0  4294967295 20069752 4294967295 4294967295 4294967295 1   1   0    0 up 0
93  6 991 0  4294967295 4294967295 4294967295 19787672  4294967295 1   1   0    0
up 0
```

Field Description:

Field	Description
prio	The priority number of the traffic policy rule.
grp	The ID of the flow control group, indicating the flow control group to which this policy belongs.
rule	Flow control policy number.
ifx	The index value of the interface to which the flow control policy rule belongs. A value of 0 indicates that the flow control group to which this rule belongs is not applied to the interface.
vlan_id	The id of the vlan-group object associated with the flow control policy rule. A value of 0 indicates that this vlan-group object is not configured.
subs_id:	The id of the subscriber object associated with the flow control policy rule. A value of 0 indicates that the subscriber object is not configured.
auth_id	The id of the auth-group object associated with the flow control policy rule. A value of 0 indicates that the auth-group object is not configured.
net_wk_id	The id of the network-group object associated with the flow control policy rule. A value of 0 indicates this network-group object.
app_id	The id of the app-group object associated with the flow control policy rule, 0 means this app-group object.
in	The id of the in-channel channel object associated with the traffic policy rule. An id value of 0 indicates that this channel object is not configured, and NA indicates that this rule is not associated with an in-channel channel object.
out	The id of the out-channel channel object associated with the traffic policy rule. An id value of 0 indicates that this channel object is not configured, and NA indicates that this rule is not associated with an out-channel channel object.
ses_now	How many flows currently match this policy rule.
ses	The maximum number of sessions allowed by the flow control policy rule to match.
stat	Down indicates that the policy is disabled, up is not disabled.

ef	The validity of the flow control policy rule, 0 means it has not taken effect yet, and 1 means it has taken effect.

【Prompt Information】-

【Platform Description】 -

4.17 small-packet

Configure small packets to go through the specified channel preferentially. Both protocols are supported without the TCP or UDP keywords

small-packet name [tcp | udp]

【Parameter Description】

Parameter	Description
name	The name of the flow channel.
TCP	Supported only, TCP, small message.
UDP	Supported only, UDP, small message.

【Default Configuration】 When the configuration is copied from the configuration template, for a dial-up port or a physical port with a bandwidth of less than or equal to 10M, by default, tcp small packets will be enabled on the upstream channel to go through the key channel.

【Command Mode】 channel-tree configuration mode

【Default Level】 14

【Usage Guide】When the egress bandwidth is small, it is recommended to enable small packets of TCP packets on the upstream channel of flow control to take priority over the key channel, which can improve the traffic throughput of applications with many small packets, such as the web.

【Configuration Example】In the "test" flow control policy group, configure tcp small packets to take priority over key channels

```
##Go to the test streaming control policy group
AC-FS(config)#flow-control test ##Go into the uplink channel tree
AC-FS(config-flow-control)#channel-tree outbound
##If there is no key channel, you will configure the key channel first
AC-FS(config-flow-control)# channel-group key parent root cir 5000 pir 10000 pri 0 per-net ##Configure tcp tabloid
message priority walk key channel
AC-FS(config-flow-control)# small-packet key tcp
```

【Prompt Information】 -

【Platform Description】 -

5 FLOW-AUDIT

5.1 flow-audit data-store

Configure the data retention days for other information tables except the daily, weekly, and monthly tables for traffic monitoring and auditing.

flow-audit data-store num

Delete related configuration.

no flow-audit data-store

【Parameter Description】

Parameter	Description
num	Unit day, the value range is 1,090 days.

【Default Configuration】 By default, it is saved for 60 days by default.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Through this command configuration, you can modify the data retention days of other information tables except the day table, week table, and month table.

【Configuration Example]】 1: Device user log on and off history report information The user feels that the record is not kept long enough, and wants to keep the record longer, configure it to 80 days.

```
AC-FS#config
Enter configuration commands, one per line. End with CNTL/Z. AC-
FS(config)# flow-audit data-store 80
```

【Verification】 1: Use the show run command to view the data retention days of other information tables except the day table, week table, and month table.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 Device support with built-in storage

5.2 flow-audit data-store day-report

Configure the number of days to retain historical data in the flow monitoring audit table.

flow-audit data-store day-report num

Delete related configuration.

no flow-audit data-store day-report

【Parameter Description】

Parameter	Description
num	Unit day, the values range from 10-90 days

【Default Configuration】 By default, the number of days to keep the historical data of the calendar is 60 days.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to configure the retention days of the historical data of the flow monitoring audit table.

【Configuration Example]】1: The hard disk is used intensively and does not want to save too much calendar data, and the configuration is 30 days.

```
AC-FS#config
Enter configuration commands, one per line. End with CNTL/Z. AC-
FS(config)# flow-audit data-store day-report 30
```

【Verification】1: Using the show run command, you can view the retention days of the historical data of the configured traffic monitoring audit day table.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 Device support with built-in storage.

5.3 flow-audit data-store month-report

Configure flow-audit data-store month-report num to retain historical data in the monthly audit table of flow monitoring. Delete the related configuration.

no flow-audit data-store month-report

【Parameter Description】

Parameter	Description
num	Unit month, the value range from January to December.

【Default Configuration】 By default, the number of months to keep the historical data of the monthly table is 12 months.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to configure the number of months to keep the historical data of the flow monitoring audit monthly table.

【Configuration Example]】1: Save too many records for one year, save them for half a year.

```
AC-FS#config
Enter configuration commands, one per line. End with CNTL/Z. AC-
FS(config)# flow-audit data-store month-report 6
```

【Verification】1: Using the show run command, you can view the number of months of historical data retention in the configuration flow monitoring and auditing monthly table.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 Device support with built-in storage

5.4 flow-audit data-store week-report

Configure the number of weeks for the retention of historical data in the flow monitoring and auditing weekly table.

flow-audit data-store week-report num

Delete related configurations.

no flow-audit data-store week-report

【Parameter Description】

Parameter	Description
num	Unit week, the values range from 1-52 weeks.

【Default Configuration】 By default, the weekly table historical data is kept for 8 weeks.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to configure the number of weeks to retain historical data in the weekly flow monitoring and auditing table.

【Configuration Example]】 1: Monitor the traffic trend of the device for a long time, but do not want to occupy too much hard disk, but do not want to record the granularity too fine, you can adjust the weekly table storage period to 28 weeks.

```
AC-FS#config
Enter configuration commands, one per line. End with CNTL/Z. AC-
FS(config)# flow-audit data-store week-report 28
```

【Verification】 1: Use the show run command to view the number of weeks of historical data retention in the configured flow monitoring and auditing weekly table.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 Device support with built-in storage.

5.5flow-audit enable

Enable the traffic monitoring and auditing function.

flow-audit enable

Disable traffic monitoring and auditing.

no flow-audit enable

【Parameter Description】-

【Default Configuration】 By default, the traffic monitoring and auditing function is enabled.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】Enable the traffic monitoring and auditing function by configuring this command.

【Configuration Example]】1: Enable the traffic monitoring and auditing function of the device.

```
AC-FS#config
AC-FS(config)# flow-audit enable
```

2: Disable the device traffic monitoring and auditing function.

```
AC-FS#config
AC-FS(config)#no flow-audit enable
```

【Verification】1: Use the show run command to monitor whether the audit function is enabled or disabled.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

5.6 flow-audit generate-report

Configure the pre-generated time point of daily report/weekly report/monthly report

flow-audit generate-report hour

Delete related configuration.

no flow-audit generate-report

【Parameter Description】

Parameter	Description
hour	In hour, the value range 0-23.

【Default Configuration】 By default, the pre-build time is 3:00 am.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to configure the pre-generated time point of daily report/weekly report/monthly report.

【Configuration Example]】 1: When the device business is busy at 3:00 am, and it is relatively idle at 5:00 am, it can be configured to generate reports at 5:00 am.

```
AC-FS#config
Enter configuration commands, one per line. End with CNTL/Z. AC-
FS(config)# flow-audit generate-report 5
```

【Verification】 1: Using the show run command, you can view the time point when the daily report/weekly report/monthly report is pre-generated.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 Device support with built-in storage.

5.7 flow-audit hard-disk-quota

Configuring Disk Quotas for Traffic Monitoring.

flow-audit hard-disk-quota percent

Delete related configuration.

no flow-audit generate-report

【Parameter Description】

Parameter	Description
Percent	Percentage, the value range 1-100.

【Default Configuration】 By default, the hard disk quota allowed for traffic monitoring is 50% of the total hard disk capacity.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 Use this command to configure the hard disk quota for traffic monitoring.

【Configuration Example]】 1: The hard disk usage of the device is tight, and 50% of the hard disk capacity for traffic auditing is too much, and I want to reduce it to 30%.

```
AC-FS#config
Enter configuration commands, one per line. End with CNTL/Z. AC-
FS(config)# flow-audit hard-disk-quota 30
```

【Verification】 1: Use the show run command to view the hard disk quota configured for traffic monitoring.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 Device support with built-in storage.

5.8 flow-audit rt-refresh

Configure the real-time traffic refresh frequency of traffic monitoring.

flow-audit rt-refresh num

Delete related configuration.

no flow-audit rt-refresh

【Parameter Description】

Parameter	Description
num	Refresh frequency, 10 seconds, no command restore default 30 seconds.

【Default Configuration】 By default, the default refresh time is 30 seconds.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】 The refresh frequency of real-time traffic can be modified through this command configuration.

【Configuration Example]】1: The device traffic monitoring real-time traffic refresh rate defaults to 30 seconds. The user thinks that the refresh rate is a bit slow and wants to see more real-time traffic information. Configure it to 10 second.

```
AC-FS#config
Enter configuration commands, one per line. End with CNTL/Z. AC-
FS(config)# flow-audit rt-refresh 10
```

【Verification】1: Use the show run command to view the set flow monitoring real-time flow refresh frequency.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

5.9 flow-audit vpn

Configure how VPN traffic is monitored.

flow-audit vpn { inside-ip | outside-ip }

【Parameter Description】-

【Default Configuration】 By default, VPN traffic monitoring is based on the external network IP.

【Command Mode】 Global configuration mode

【Default Level】 14

【Usage Guide】Through this command configuration, the monitoring mode of VPN traffic can be modified, and the user can configure it according to actual needs.

【Configuration Example]】1: The company headquarters acts as the VPN server, and wants to check the IP traffic of each branch (dial-up through VPN).

```
AC-FS#config
Enter configuration commands, one per line. End with CNTL/Z. AC-
FS(config)# flow-audit vpn outside-ip
```

2: The branch office is used as a VPN client, and if you want to see the traffic of each employee in the branch accessing VPN resources, you need to modify it to monitor based on the intranet IP.

```
AC-FS#config
Enter configuration commands, one per line.  End with CNTL/Z.
AC-FS(config)# flow-audit vpn inside-ip
```

【Verification】1: Use the show run command to view the configured VPN monitoring mode.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

5.10 show flowrate

Displays the current traffic information of the whole machine or specified interface within a certain period of time or within the last few hours.

show flowrate { global | interface interface-name } [{ recent hour | minute_interval begin-year begin-month begin-day begin-hour:begin-minute to end-year end-month end-day end-hour:end-minute | [month | week] time-interval begin-year begin-month begin-day begin-hour to end-year end-month end-day end-hour | { [month | week] day-interval begin-year begin-month begin -day to end-year end-month end-day | day begin-year begin-month begin-day } [hour-interval begin-hour to end-hour [begin-hour2 to end-hour2]] } [detail]]

【Parameter Description】

Parameter	Description

interface-name	Interface name.
hour	Number of hours in recent days.
begin-year	The starting year of the time period.
begin-month	Time period starting month.
begin-day	Start date of time period.
begin-hour	Time period start hours.
begin-minute	Time period starting minutes.
end-year	The end of the time period.
end-month	Time period end month.
end-day	End date of time period.
end-hour	Time period end hours.
end-minute	Time period ends minutes.
begin-hour2	Time period starting hour 2.
end-hour2	Time period end hour 2.

【Default Configuration】 None.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Display the real-time traffic information of the whole machine or specified interface.

Display the real-time traffic information of the whole machine by specifying the keyword global; display the real-time traffic information under the specified interface by specifying the keyword interface;

eg: show flowrate global (query real-time flow rate information of the whole machine).

show flowrate interface gi0/3 (queries the real-time traffic information under the channel name "gi0/3").

【Configuration Example】1: Display the current traffic of interface gigabitEthernet 0/1.

```
AC-FS# show flowrate interface gigabitEthernet 0/1
Interface: GigabitEthernet 0/1
Pass input rate: 979685 bits/sec, 114 packets/sec
Pass output rate: 107233 bits/sec, 60 packets/sec
Drop input rate: 130 bits/sec, 5 packets/sec
Drop output rate: 210 bits/sec, 4packets/sec
```

2: Display the real-time traffic information of the whole machine.

```
AC-FS# show flowrate global
global
Pass Input rate:          184592 bits/sec,              33 packets/sec
Pass Output rate:          30940 bits/sec,              28 packets/sec
Drop Input rate:               0 bits/sec,              0 packets/sec
Drop Output rate:              0 bits/sec,              0 packets/sec
```

【Prompt Information】 -

【Platform Description】 Over time period, only supported by devices with built-in storage.

5.11 show flowrate application

Displays the traffic information related to the application, application group, and application type in the current or time period of the whole machine or the specified channel.

show flowrate application { global | interface interface-name | vwan } [[subscriber subscriber-name] [subscriber-group subscriber-group] | { by-auth } [auth-subs-group auth-group-name] [auth-subs auth-name]] [ip ip-address] [application-group application-group] [{ [by-group] | [application-type application-type] [{ by-type | application application-name }] }] [{ recent hour | minute-interval begin-year begin-month begin-day begin-hour:begin-minute to end-year end-month end-day end-hour:end-minute | { [month | week] day-interval begin-year begin-month begin-day to end-year end-month end-day | day begin-year begin-month begin-day } [hour-interval begin-hour1 to end-hour1

[begin-hour2 to end-hour2] }] [order-by { { pass | drop } { upload | download } | application } { desc |

asc } [top n]] [detail]

【Parameter Description】

Parameter	Description
interface-name	Three-tier interface name, used in gateway mode.
subscriber-name	user name.
subscriber-group	User group name.
auth-group	Certified Object Group Name.
auth-name	Certified Object Name.
Ip-address	IP address.
application-group	Application group name.
application-type	Application type.
application-name	Apply names.
hour	Number of hours in recent days.
begin-year	The starting year of the time period.

begin-month	Time period starting month.
begin-day	Start date of time period.
begin-hour	Time period start hours.
begin-minute	Time period starting minutes.
end-year	The end of the time period.
end-month	Time period end month.
end-day	End date of time period.
end-hour	Time period end hours.
end-minute	Time period ends minutes.
begin-hour1	Time period start hour 1.
end-hour1	Time period end hour 1.
begin-hour2	Time period starting hour 2.
end-hour2	Time period end hour 2.
n	The first n record.

【Default Configuration】 None.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Display application-related real-time traffic information.

1. Display the real-time traffic information of the whole machine application, application group and application type by specifying the keyword global; display the real-time traffic information of the application, application group and application type under the specified interface by specifying the keyword interface; display the pipeline by specifying the keyword vwan Accelerate the real-time traffic information of application, application group and application type; query the real-time traffic information of the application without entering any filter conditions; query the real-time traffic information of the application group by specifying the keyword by-group; specify the keyword by- type queries the real-time traffic information of the application type.

eg: show flowrate application global (query the real-time application flow information of the whole machine).

show flowrate application interface gi0/3 (query the real-time flow information of various applications under the channel name "gi0/3")

show flowrate application interface gi0/3 by-group (query all application groups under the channel name "gi0/3" real-time traffic information).

show flowrate application interface gi0/3 by-type (queries the real-time traffic information of all application types under the channel name "gi0/3").

show flowr app vwan (queries the real-time flow of the pipeline acceleration application).

2. Display the first n records of the sorting result through the keywords top and Parametern;

eg: show flowrate application interface gi0/3 order by pass download desc top 5 (Query the real-time application traffic under the channel name "gi0/3", the results are sorted in descending order by download traffic, and the top 5 records are displayed).

3. Query real-time application traffic information by filtering one or more of the keywords subscriber, subscriber-group, auth-subs-group, auth-subs, ip.

eg: show flowrate application interface gi0/3 ip 192.168.1.5 (the ip under the query channel name "gi0/3" is 192.168.1.5 of real-time application traffic,).

This command supports the function of collecting statistics by group: you can use the keywords by-group and by-type to realize the function of collecting statistics by application group and application type. The command also supports the display results in ascending and descending order according to the passed and discarded upstream and downstream traffic and application name;

【Configuration Example】 1: In gateway mode, display the current application traffic of interface gigabitEthernet 0/1.

```
AC-FS# show flowrate application interface gigabitEthernet 0/1 path:GigabitEthernet 0/1
count: 1
Application    Application-group Application-type
PASS:  Upload(bps)  Download(bps)  Upload(pps)  Download(pps) DROP: Upload(bps) Download(bps) Upload(pps)
Download(pps)
App1          instant message software   other application group
62597     65955          15      17
0            0            0            0
```

2: Display the real-time application traffic information of the whole machine.

```
AC-FS# show flowr app global global
count: 4
Application    Application-group   Application-type
PASS:  Upload(bps)  Download(bps)  Upload(pps)  Download(pps) DROP: Upload(bps) Download(bps) Upload(pps)
Download(pps)
Tencent resources              P2P APP     Unkey_Group
211              249          0            0
0                  0            0            0 QQ-Loginl|chat          instant message software      Key_Group
286              373          0                  0
0            0            0            0 IP application                  IP  protocol suite        Other_Group 20014 70481       12
12
0            0            0            0 telnet    remote access protocol     Other_Group
64           153                  0            0
0            0                  0                  0
```

3: Display pipeline acceleration real-time application traffic information.

```
AC-FS# show flowr app vwan vwan
count: 3
Application    Application-group   Application-type
PASS:  Upload(bps)  Download(bps)  Upload(pps)  Download(pps) DROP: Upload(bps) Download(bps) Upload(pps)
Download(pps)
Tencent resources              P2P APP    Unkey_Group
786          565          0          0
0            0            0          0 QQ-Login|chat   instant message software    Key_Group
211          373          0          0
0            0            0          0 IP application    IP protocol suite    Other_Group 20014 70481       12     12
0            0            0          0
```

【Prompt Information】-

【Platform Description】 Over time period, only supported by devices with built-in storage.

5.12 show flowrate ip

Displays the current traffic information of the whole machine or specified interface within a certain period of time or within the last few hours.

show flowrate ip { global | { interface interface-name} [by-vpn] | vwan }

[subscriber-group subscriber-group by-group | [[subscriber-group subscriber-group] [subscriber subscriber-name] [vip] | { by-auth } [auth-subs-group auth-group-name] [auth- subs auth-name]] [ip ip-address] [application application-name] [application-group application-group] [application-type application-type]] [{ recent hour | minute-interval begin-year begin-month begin -day begin-hour:begin-minute to end-year end-month end-day end-hour: end-minute | { [month | week] day-interval begin-year begin-month begin-day to end-year end -month end-day | day begin-year begin-month begin-day } [hour-interval begin-hour1 to end-hour1 [begin-hour2 to end-hour2]] }] [order-by { { pass | drop } { upload | download } | ip | subscriber- group | subscriber | auth-subs-group | auth-subs } { desc | asc } [top n [detail]]] [{ detail | by-user }]

【Parameter Description】

Parameter	Description
interface-name	Interface name, used in gateway mode.
subscriber-group	User group name.
subscriber-name	User name.
auth-group	Certified Object Group Name.
auth-name	Certified Object Name.

Ip-address	IP address.
application-name	Apply names.
application-group	Application group name.
application-type	Application type.
hour	Number of hours in recent days.
begin-year	The starting year of the time period.
begin-month	Time period starting month.
begin-day	Start date of time period.
begin-hour	Time period start hours.
begin-minute	Time period starting minutes.
end-year	The end of the time period.
end-month	Time period end month.
end-day	End date of time period.
end-hour	Time period end hours.
end-minute	Time period ends minutes.
begin-hour1	Time period start hour 1.
end-hour1	Time period end hour 1.
begin-hour2	Time period starting hour 2.
end-hour2	Time period end hour 2.
n	The first n record.

【Default Configuration】 None.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Displays real-time traffic information related to users.

1. Specify the keyword global to display the real-time traffic information of the user of the whole machine; specify the keyword interface to display the real-time traffic information of the user under the specified interface; specify the keyword vwan to display the real-time traffic information of the pipeline acceleration user.

eg: show flowrate ip global (to query the real-time traffic information of users on the whole machine).

show flowrate ip interface gi0/3 (queries the real-time traffic information of users under the channel name "gi0/3").

show flowrate ip vwan (queries the real-time traffic information of users who take the pipeline to accelerate).

2. Get the top n records of the sorting result through the keywords top and Parametern;

eg: show flowrate ip interface gi0/3 order by pass download desc top 5 (query the real-time user traffic under the channel name "gi0/3", the results are sorted in descending order by download traffic, and the top 5 records are displayed).

3. Filter and query real-time application traffic information by one or more of the keywords application, application-group, and application-type.

eg: show flowrate ip interface gi0/3 application PPTP (to query the real-time user traffic whose app is PPTP under the channel name "gi0/3")

This command supports the function of statistics by group, you can use the by-group keyword to realize the function of statistics by user group.

【Configuration Example】 1: In gateway mode, display the current user traffic of interface gigabitEthernet 0/1.

```
AC-FS# show flowrate ip interface gigabitEthernet 0/1
Subscriber                  ip
PASS: Upload(bps)   Download(bps)    Upload(pps)    Download(pps)
DROP: Upload(bps)   Download(bps)   Upload(pps)   Download(pps)
/User_groupA/User_nameA 2.2.2.92
230                 134                 0                   0
0                   0                   0                   0
/User_groupB/User_nameB  172.18.3.67
259                 153                 0                   0
0                   0                   0                   0
```

2: Display the real-time user traffic of the whole machine.

```
AC-FS# show flowr ip global
global
subscriber           ip
PASS: Upload(bps)   Download(bps)    Upload(pps)    Download(pps)
DROP: Upload(bps)   Download(bps)   Upload(pps)   Download(pps)
/172.18.3.24        172.18.3.24
896                   1008                  1                     1
0                     0                     0                     0
/172.18.3.110        172.18.3.110
7526                  63712                 9                     9259
0                     0                     0                     0
/192.168.183.118        192.168.183.118
18116                 68729                 10                    10
0                     0                     0                     0
```

【Prompt Information】 -

【Platform Description】 Over time period, only supported by devices with built-in storage.

5.13 show flowrate ip-application

Display the real-time traffic information of IP and application under the whole machine or specified channel.

show flowrate ip-application { global | interface interface-name [by-vpn] } [[subscriber subscriber-name] [subscriber-group subscriber-group] [vip] | { by-auth } [auth-subs-group auth- group-name] [auth-subs auth-name]] [ip ip-address] [application application-name] [application-group application-group] [application-type application-type] [order-by { { pass | drop } { upload | download } | ip | application | subscriber-group | subscriber | auth-subs-group | auth-subs } {desc | asc } [top n]]

【Parameter Description】

Parameter	Description
interface-name	Interface name, used in gateway mode
subscriber-group	User group name
subscriber-name	user name
auth-group-name	Certified Object Group Name
auth-name	Certified Object Name
ip-address	IP address
application-name	apply names
application-group	application group name
application-type	Application type
n	The first n record

【Default Configuration】 None.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Displays real-time traffic information related to ip and application.

1. Display the real-time traffic information of the whole machine IP and application by specifying the keyword global; display the real-time traffic information of the IP and application under the specified interface by specifying the keyword interface;

eg: show flowrate ip-application global ip 192.168.1.3 (queries the whole machine IP and application information).

show flowrate ip-application interface gi0/3 ip 192.168.1.3 (the query channel name is "gi0/3" and the ip is 192.168.1.3 IP, application traffic information).

2. Display the first n records of the sorting result through the keywords top and Parameter n;

eg: show flowrate ip-application interface gi0/3 ip 192.168.1.3 order by pass download desc top 5 (Query the current application traffic

whose ip is 192.168.1.1 under the channel name "gi0/3", and the results are sorted in descending order of download traffic, and show first 5 records).

【 **Configuration Example** 】 1: In gateway mode, display the application traffic whose IP address is 172.18.36.102 on interface gigabitEthernet 0/1.

```
AC-FS# show flowrate ip-application interface gigabitEthernet 0/1
ip 172.18.36.102
path:GigabitEthernet 0/1
Subscriber  ip  Application   Application-group   Application-type
PASS:  Upload(bps)   Download(bps)     Upload(pps)     Download(pps)
DROP:  Upload(bps)   Download(bps)   Upload(pps)   Download(pps)
/user_groupA/user_nameA  172.18.36.102   applicationA   application_groupA     application groups
46003               2093107             93                  173
0                   0                   0                   0
/user_groupA/user_nameB 172.18.36.102  applicationB  application_groupB   application
groups
46001               2093102             193                  173
0                   0                   0                   0
/user_groupA/user_nameC172.18.36.102  applicationC application_groupC   application
groups4003               1093107             63                  73
0                   0                   0                   0
```

【**Prompt Information**】-

【**Platform Description**】 Over time period, only supported by devices with built-in storage

5.14 show online ip

Display the Internet access time, traffic information and IP Internet access time information of the current online IP under the whole machine or the specified channel.

show online ip {global | interface interface-name} [[subscriber subscriber-name] [subscriber-group subscriber-group] [vip] | [auth auth-name] [auth-group auth-group]] [ip ip-address] [{minute-interval begin-year begin-month begin-day begin-hour: begin-minute to end-year end-month end-day end-hour:end-minute | {[month | week] day-interval begin -year begin-month begin-day to end-year end-month end-day | day begin-year begin-month begin-day} [hour-interval begin-hour to end-hour [begin-hour2 to end-hour2]]}] [order-by {{pass | drop} {upload | download} | ip | subscriber-group | subscriber | auth-group | auth } {desc | asc}[top n]]

【**Parameter Description**】

Parameter	Description
interface-name	Three-tier interface name, used in gateway mode.

subscriber-name	user name.
subscriber-group	User group name.
auth-name	Certified Object Name.
auth-group	Certified Object Group Name.
Ip-address	IP address.
begin-minute	Time period starting minutes.
end-minute	Time period ends minutes.
begin-day	Start date of time period.
begin-month	Time period starting month.
begin-year	The starting year of the time period.
end-day	End date of time period.
end-month	Time period end month.
end-year	The end of the time period.
begin-hour	Time period start hours.
end-hour	Time period end hours.
begin-hour2	Time period starting hour 2.
end-hour2	Time period end hour 2.
n	The first n record.

【Default Configuration】 None.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Displays the online time and traffic information related to the online IP.

1. Display the real-time online IP traffic information of the whole machine by specifying the keyword global;

eg: show online ip global (to query the current online IP traffic information of the whole machine).

2. Display the top n records sorted by the keywords top and Parameter n;

eg: show online ip global order by pass download desc top 5 (queries the current online IP traffic of the whole machine, the results are sorted in descending order by download traffic, and the first 5 records are displayed).

【Configuration Example]】1: Display the online users' duration and traffic information, and sort them by download traffic, and display the top 5.

```
AC-FS# show online ip global order-by pass download desc top 5
global
Subscriber
IP                  AuthType      LoginTime           OnlineTime(min) PASS-
Upload(KB)  PASS-Download(KB)  DROP-Upload(KB)  DROP-Download(KB)
/200.200.0.6
200.200.0.6                             2013-7-3 15:38 1345
1405491             655083              0                   0
/200.200.0.7
200.200.0.7                             2013-7-3 15:38 1345
1405489             655044              0                   0
/200.200.0.8
200.200.0.8                             2013-7-3 15:38 1345
1405128             655016              0                   0
/200.200.0.2
200.200.0.2                             2013-7-3 15:38 1345
1405221             654959              0                   0
/200.200.0.9
200.200.0.9                             2013-7-3 15:38 1345
1404516             654826              0                   0
```

【Prompt Information】-

【Platform Description】 Over time period, only supported by devices with built-in storage.

5.15 show online ip-application

Displays the current online IP, application duration, and traffic information of the entire machine or the specified channel.

show online ip-application {global | interface interface-name} [[subscriber subscriber-name] [subscriber-group subscriber-group] [vip] | [auth auth-name] [auth-group auth-group]] [ip ip -address] [application application-name] [application-group application-group] [application-type application-type] [order-by {{pass | drop} {upload | download} | ip | subscriber-group | subscriber | auth -group | application} {desc | asc}] [offset start –record {limit record-num}]

【Parameter Description】

Parameter	Description
interface-name	Three-tier interface name, used in gateway mode.
subscriber-name	User name.
subscriber-group	User group name.
auth-name	Certified Object Name.

auth-group	Certified Object Group Name.
Ip-address	IP address.
application-name	Apply names.
application-group	Application group name.
application-type	Application type.
start-record	Offset the record line.
record-num	The number of record lines displayed.

【Default Configuration】 None.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 By specifying the keyword global, it can display the current online IP of the whole machine, the duration of the Internet access of the application, and the traffic information. Use the keywords ip, subscriber, subscriber-group, application, application-group to achieve conditional filtering, use the keyword order-by to specify the sort order of query results; use top n to display the top n records

【Configuration Example]】 1: Display the online duration and traffic information of the IP application whose IP address is 172.18.181.63.

```
AC-FS# show online ip-application global ip 200.200.0.2
global
count:2
Subscriber
IP                 Application Application-group Application-type
LoginTime          OnlineTime(min)
PASS-Upload(KB)    PASS-Download(KB)    DROP-Upload(KB)      DROP-Download(KB)
/172.18.181.63
 172.18.181.63          BQQ  Instant message software    Other_Group
 2013-8-26 9:36           10456
   16703               28711               0                   0
/172.18.181.63
 172.18.181.63          MAPI    MAPI E-mail protocol Other_Group
 2013-8-26 9:36           10456
   5107                8231                0                   0
```

【Prompt Information】 -

【Platform Description】 Over time period, only supported by devices with built-in storage

5.16show online statistic

Display the number of IPs and sessions currently online on the whole machine or under the specified channel, within the last hour or within the specified time period.

show online statistics {global | interface interface-name} [{detail [offset start-record {limit record-num}] | recent hour | minute-interval begin-year begin-month begin-day begin-hour:begin-minute to end-year end-month end-day end-hour:end-minute | [month | week] time-interval begin-year begin-month begin-day begin-hour to end-year end-month end-day end-hour | day begin-year begin-month begin-day [hour-interval begin-hour1 to end-hour1 [begin-hour2 to end-hour2]]}]

【Parameter Description】

Parameter	Description
interface-name	Three-tier interface name, used in gateway mode.
start-record	Offset the record line.
record-num	The number of record lines displayed.
hour	Number of hours in recent days.
begin-year	The starting year of the time period.
begin-month	Time period starting month.
begin-day	Start date of time period.
begin-hour	Time period start hours.
begin-minute	Time period starting minutes.
end-year	The end of the time period.
end-month	Time period end month.
end-day	End date of time period.
end-hour	Time period end hours.
end-minute	Time period ends minutes.
begin-hour	Time period start hours.
end-hour	Time period end hours.
begin-hour2	Time period starting hour 2.
end-hour2	Time period end hour 2.

【Default Configuration】 None.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Display the total number of current online ip.

Display the total number of current online IPs of the whole machine by specifying the keyword global.

eg: show online statistics global (to query the total number of current online IPs).

【Configuration Example】1: Display the current total IP of the whole machine.

```
AC-FS# show online statistics global
global
online ip count: 500
```

【Prompt Information】-

【Platform Description】 Over time period, only supported by devices with built-in storage.

6 CONTENT-AUDIT

6.1 app-audit

Enable the optimized audit function of application blocking and set the interval time.

app-audit optimize-cache [time]

Turn off the optimized auditing function of application blocking.

no app-audit optimize-cache

Enable application control auditing to optimize blocking of TCP connections, that is, actively send rst packets to disconnect connections.

app-audit optimize-deny

Disable the optimized blocking function of TCP connections by application control auditing.

no app-audit optimize-deny

【Parameter Description】

Parameter	Description
time	The unit of this parameter is seconds. After this function is enabled, the audit of the same IP within the time period will not be repeated.

【Default Configuration】 It is enabled by default.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 1: After the optimization audit function is enabled, the same application blocking action of the same IP within a certain period of time will not be audited repeatedly. The default length of time is 300s, the range is 5~1800s.

2: For TCP flow, there are two ways to apply blocking: one is to directly lose packets, and the other is to actively disconnect by sending rst packets. These two ways can be switched by optimizing the blocking configuration.

【Configuration Example]】 1: Within the specified 120s, the duplicate application blocking of the same IP will not be audited.

```
AC-FS# configure terminal
AC-FS(config)# app-audit optimize-cache 120 AC-
FS(config)# end
```

2: Disable the optimization blocking function of application control auditing.

AC-FS# configure terminal

```
AC-FS(config)# no app-audit optimize-deny
AC-FS(config)# end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.2 app-rule

Delete all application control audit rules under the policy group.

app-rule delete-all

Exchange the priority of access control rules.

app-rule priority-swap rule-id1 rule-id2

Add application control audit rules to the content audit policy group.

app-rule rule-id time-range time-name app-group app-group-name action { permit | deny } [audit] [vpn] [vip] [comment comment-string]

Delete application control audit rules.

no app-rule rule-id

【Parameter Description】

Parameter	Description
rule-id1	The ID of Rule 1 for the priority level to be exchanged.
rule-id2	The ID of Rule 2 for the priority level to be exchanged.
rule-id	ID identification of the rule, value range (1~200), and rule capacity of 200.
time-name	Time object name that represents the rule effective time period.
app-group-name	The application group name that the rule wants to control.

comment-string	Description of the rule.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Content audit policy group configuration mode

【Default Level】 14

【Usage Guide】 1: The rule-id of a rule is not allowed to be repeated in the same content audit policy group, but is allowed to be repeated in different content audit policy groups.

2: The access control rules in a content audit policy group have corresponding priorities, and the rule assigned last has the highest priority.

3: The time-name and app-group-name associated with the rule may not exist, and the rule will not take effect at this time.

4: When configured to allow application access and auditing, restrictions will be imposed to optimize audit records. In fact, no auditing is performed in this case.

5: The swap priority command is used to swap the priorities of two access control rules. After running this command, you can see that the order of the two rules has changed in show running-config, but the order of the two rules will not appear in show running-config. Order.

【Configuration Example]】 1: Delete all application control audit rules in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# app-rule delete-all
AC-FS(cont-plcy-config)# end
```

2: The priority of the application control audit rule 10 and rule 20 in the exchange policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# app-rule priority-swap 10 20
AC-FS(cont-plcy-config)# end
```

3: Add an application control audit rule to the policy group policyA, filter users for video playback and P2P download, and audit the corresponding filtering information.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# app-rule 2 time-range any direction double app-group VideoAndP2PGroup
action deny audit comment DenyVideoAndP2P
AC-FS(cont-plcy-config)# end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】1: If the configured rule-id already exists, a prompt will be given.

```
AC-FS(config)# app-rule 2 time-range any direction double app-group VideoAndP2PGroup action deny
audit comment DenyVideoAndP2P
Rule 2 already exists, please delete it first
```

【Common Mistake】-

【Platform Description】 -

6.3class

Add the contained URL categories to the URL object.

class class-name

Deletes the URL category contained in the URL object.

no class class-name

【Parameter Description】

Parameter	Description
class-name	The name of the URL classification, which can be the user-defined URL classification, or which comes from the system URL classify. The maximum length is 40 bytes.

【Default Configuration】 There is no configuration by default.

【Command Mode】 URL object configuration mode

【Default Level】 14

【Usage Guide】 1: The URL object allows to include system URL categories and user-defined URL categories.

2: The URL object allows to associate non-existing URL categories.

【Configuration Example]】1: Add a URL category named classA to the URL object objA.

```
AC-FS# configure terminal AC-
FS(config)# url-object objA AC-
FS(url-obj-config)# class classA
AC-FS(url-obj-config)# end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.4clear content-audit statistics

Clear real-time statistics for content auditing.

clear content-audit statistics

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to clear the real-time statistics of content auditing.

【Configuration Example]】1: Clear the real-time statistics of content auditing.

```
AC-FS#clear content-audit statistics
```

【Prompt Information】-

【Platform Description】 -

6.5comment

Add a Description to a URL category or URL object.

comment comment-string

Delete the Description from the URL category or URL object.

no comment

【Parameter Description】

Parameter	Description
comment-string	Description for a URL classification or URL object with up to 100 characters.

【Default Configuration】 There is no configuration by default.

【Command Mode】URL object configuration mode, URL classification configuration mode

【Default Level】 14

【Usage Guide】 Description is usually used to describe the purpose of URL category or URL object.

【Configuration Example]】1: Add a Description to the URL object objA.

```
AC-FS# configure terminal AC-
FS(config)# url-object objA
AC-FS(url-obj-config)# comment OBJA-COMMENT
AC-FS(url-obj-config)# end
```

2: Add a Description to the URL category classA.

```
AC-FS# configure terminal AC-
FS(config)# url-class classA
AC-FS(url-cls-config)# comment CLASSA-COMMENT
AC-FS(url-cls-config)# end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.6 content-audit http-port

Add an HTTP port.

content-audit http-port port-num

Remove an HTTP port.

no content-audit http-port port-num

【Parameter Description】

Parameter	Description
port-num	Port number, range: 1~65535, of which 80 and 8080 are default ports of the system, and users are not allowed to configure or delete them.

【Default Configuration】 None.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】When the application identification is not enabled, when a website needs to be audited, but the port is not 80 or 8080, you can use this command to add the port of this website to the HTTP port, and the website can be audited.

【Configuration Example]】1: Add port 60000 as the HTTP port.

```
AC-FS# configure terminal
AC-FS(config)# content-audit http-port 60000
AC-FS(url-obj-config)# end
```

2: Remove port 60000 from HTTP ports.

```
AC-FS# configure terminal
AC-FS(config)# no content-audit http-port 60000
AC-FS(url-obj-config)# end
```

【Verification】Use the show content-audit http-port or show running-config command to view the configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.7 content-audit https-port

Add an HTTPS port.

content-audit https-port port-num

Remove an HTTPS port.

no content-audit https-port port-num

【Parameter Description】

Parameter	Description
port-num	Port number, range: 1~65535, of which 443 is the default port of the system, and users are not allowed to configure or delete it.

【Default Configuration】 None.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】When the application identification is not enabled, when an HTTPS encrypted website needs to be audited, but the port is not 443, you can use this command to add the port of this website to the HTTPS port, and the website can be audited.

【Configuration Example]】1: Add port 4430 as the HTTPS port.

```
AC-FS# configure terminal
AC-FS(config)# content-audit https-port 4430
AC-FS(url-obj-config)# end
```

2: Remove port 4430 from HTTP ports.

AC-FS# configure terminal

```
AC-FS(config)# no content-audit https-port 4430
AC-FS(url-obj-config)# end
```

【Verification】Use the show content-audit https-port or show running-config command to view the configuration information.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.8 content-audit write-db

Turn on the switch of writing the audit information of each business in the content audit to the local storage.

content-audit write-db { url | web-search | web-bbs | web-mail | mail | im | app-control | vid }

Turns off the switch for writing the audit information of each business in the content audit to the local storage.

no content-audit write-db { url | web-search | web-bbs | web-mail | mail | im | app-control | vid }

【Parameter Description】-

【Default Configuration】 ACE product: application control auditing (app-control) is enabled by default, other services are disabled by default; other products: all services are enabled by default.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】When the audit information of each business of the content audit is sent to the external log server, this switch can be turned off, and the database will not be written locally, reducing the burden on the device.

【Configuration Example]】1: Enable the switch of writing url audit information to local storage.

```
AC-FS# configure terminal
AC-FS(config)# content-audit write-db url
AC-FS(url-obj-config)# end
```

2: Turn off the switch for writing url audit information to local storage.

```
AC-FS# configure terminal
AC-FS(config)# no content-audit write-db url
AC-FS(url-obj-config)# end
```

【Verification】Use the show content-audit write-db/show running-config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 Products with built-in storage are supported, products without built-in storage are not supported.

6.9 content-object

Specify the content object name and enter the content object configuration mode.

content-object object-name

Deletes the content object, and any keywords it contains.

no content-object object-name

【Parameter Description】

Parameter	Description
object-name	Content object name. The maximum length is 40 bytes.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Use this command to configure the content object. The content object capacity is 100.

【Configuration Example]】1: Configure a content object objA, including the keyword hello and the regular match .ietf.org.

```
AC-FS#  configure  terminal AC-FS(config)#
content-object objA AC-FS(content-obj-
config)# keyword hello
AC-FS(content-obj-config)# regexp .*\.ietf\.org
AC-FS(content-obj-config)# end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.10 content-policy

Specify the content audit policy group name and enter the content audit policy group configuration mode.

content-policy policy-name

Delete the content audit policy group, and all the rules it contains.

no content-policy policy-name

【Parameter Description】

Parameter	Description
policy-name	The Content Audit Policy Group name. The maximum length is 100 bytes.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Use this command to configure policy groups. The policy group has a capacity of 100.

【Configuration Example]】1: Configure a content audit policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.11 content-policy-config

Globally disable custom policy groups.

content-policy-config disable-all

Cancel the global disable of the custom policy group.

no content-policy-config disable-all

Disable a policy group.

content-policy-config disable-policy policy-name

Un-disable the policy group.

no content-policy-config disable-policy policy-name

Swap the priorities of the two policy groups.

content-policy-config priority-swap policy-name1 policy-name2

【Parameter Description】

Parameter	Description
policy-name	Content audit policy group name.
policy-name1	The name of the policy group whose priority needs to be swapped.
policy-name2	Another policy group name whose priority needs to be reversed.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 1: Global disable only works for custom policy groups, not for built-in policy groups.

2: The policy group is valid by default. Disabling a policy group provides a way to retain a policy group configuration, but not use the policy group. To disable a policy group, you need to explicitly configure a disable command.

3: Disabling a policy group does not delete the policy group content and association with the user.

4: When configuring the disable policy group command, if the specified policy group name does not exist, the command will not take effect.

5: After the policy group is deleted, the disabled policy group configuration will also be deleted at the same time.

6: After configuring and exchanging the priorities of the two policy groups, you can see that the order of the two policy groups has changed in show running-config, but this command will not appear in show running-config.

【Configuration Example]】1: Close all custom policy groups.

```
AC-FS# configure terminal
AC-FS(config)# content-policy-config disable-all
AC-FS(config)# end
```

2: Disable the content audit policy group policyA.

AC-FS# configure terminal

```
AC-FS(config)# content-policy-config disable-policy policyA
AC-FS(config)# end
```

3: Exchange the priorities of the two policy groups policyA and policyB.

```
AC-FS# configure terminal
AC-FS(config)# content-policy-config policy-swap policyA policyB AC-FS(config)#
end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.12 content-policy-relate

Sets the policy that users do not inherit the parent user group.

content-policy-relate no-inherit { subscriber { subs-name1 | any } | auth-subscriber { subs-name2 | any } }

Restores the user's policy inheritance properties.

no content-policy-relate no-inherit { subscriber { subs-name1 | any } | auth-subscriber { subs-name2 | any } }

Associate policy groups to users.

content-policy-relate relate { subscriber { subs-name1 | any } | auth-subscriber { subs-name2 | any } } policy policy-name

Remove the user's association with the policy group.

no content-policy-relate relate { subscriber { subs-name1 | any } | auth-subscriber { subs-name2 | any } } policy policy-name

【Parameter Description】

Parameter	Description
subs-name1	Static user associated with the policy group. The Internet cafe version of the NBR products can also be associated with custom user groups.
subs-name2	The authentication user associated with the policy group.
policy-name	Policy group name.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】1: When configuring the user's policy inheritance attribute, the specified user subs-name1 and subs-name2 may not exist. If there is a policy association at this time, the command can exist, but the rule does not take effect. After a user is removed from all policy groups, the user's Disable Policy Inheritance property is also removed.

2: When configuring an association rule, if the policy group name does not exist, the association operation will not take effect and the command will not exist.

3: When configuring an association rule, the associated users subs-name1 and subs-name2 may not exist. At this time, the command can exist, but the rule does not take effect.

4: When configuring association rules, subscriber or auth-subscriber can specify multiple user names, separated by commas, indicating that multiple users are associated with the policy group. policy-name also allows specifying multiple policy groups, separated by commas.

【Configuration Example]】1: Configure static user user1 not to inherit the policy of its parent user group.

```
AC-FS# configure terminal
AC-FS(config)# content-policy-relate no-inherit subscriber user1 AC-FS(config)#
end
```

2: Configure a content audit policy group named policyA to associate with the static users user1 and user2, and also associate policyA and policyB with the authentication user auth-user3. Configure a policy group named policyC associated with the custom user group cstm_grp1.

```
AC-FS# configure terminal
AC-FS(config)# content-policy-relate relate subscriber usr1,user2 policy policyA AC-FS(config)#
content-policy-relate relate auth-subscriber auth-user3 policy policyA,policyB AC-FS(config)#
content-policy-relate relate subscriber cstm_grp1 policy policyC AC-FS(config)# end
```

【Verification】 Use the show running-config command to view the configuration status.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

6.13 https-audit enable

Enable HTTPS auditing.

https-audit enable

Disable HTTPS auditing.

no https-audit enable

【Parameter Description】 -

【Default Configuration】 It is disabled by default.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 It must be used in conjunction with the rules of each sub-service of content auditing. For example, after enabling the HTTPS audit enable switch, you need to configure URL rules to perform domain name auditing and filtering on HTTPS encrypted websites.

【Configuration Example]】 1: Enable the HTTPS audit function.

```
AC-FS# configure terminal AC-
FS(config)# https-audit enable
AC-FS(config)# end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.14im-rule

Enable IM default auditing.

im-rule audit-default-enable

Disable the default audit function of IM.

no im-rule audit-default-enable

Delete all IM rules under the policy group.

im-rule delete-all

Exchange the priority of IM access control rules.

im-rule priority-swap rule-id1 rule-id2

Add the public section of IM access control rules to the content audit policy group.

im-rule rule-id time-range time-name action { permit | deny } [audit] [comment comment-string]

Add a further ParameterDescription of the IM access control rule to the content audit policy group, mainly the keyword matching conditions of the Description rule. This command must be used in conjunction with the im-rule rule-id time-range command.

im-rule rule-id im-type im-name [relation { and | or } [account content-object-name1] [message

content-object-name2]]

Delete IM access control rules.

no im-rule rule-id

【Parameter Description】

Parameter	Description

rule-id1	The ID of rule 1 whose priority is to be exchanged.
rule-id2	ID of rule 2 whose priority is to be exchanged.
rule-id	The ID of the rule, the value range (1~200), and the rule capacity is 200.
time-name	The name of the time object representing the effective time period of the rule.
comment-string	Description of the rule.
im-name	Specifies the audited IM software. im-name represents a specific string string. For example, if the string is "qq", it means that this rule only audits QQ software; if the string is "qq,msn" or "msn,qq", it means that this rule only audits QQ software and MSN software.
content-object-name1	IM account, if this item is missing, it means that this item does not need to be matched.
content-object-name2	Chat history, if this item is missing, it means that this item does not need to be matched.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Content audit policy group configuration mode

【Default Level】 14

【Usage Guide】 1: The rule-id of a rule is not allowed to be repeated in the same content audit policy group, but is allowed to be repeated in different content audit policy groups.

2: The access control rules in a content audit policy group have corresponding priorities, and the rule assigned last has the highest priority.

3: The time-name and content-object-name associated with the rule may not exist, and the rule will not take effect at this time.

4: QQ chat is encrypted information and currently does not support content filtering and auditing (if im-name is QQ, message cannot be configured).

5: The swap priority command is used to swap the priorities of two access control rules. After running this command, you can see that the order of the two rules has changed in show running-config, but the order of the two rules will not appear in show running-config. Order.

6: The default audit can only be configured in the default audit group whose policy group name is _AUDIT_DEFAULT, and this command will not take effect if configured in other policy groups.

【Configuration Example]】 1: Enable IM default auditing.

```
AC-FS# configure terminal
AC-FS(config)# content-policy _AUDIT_DEFAULT AC-
FS(cont-plcy-config)# im-rule audit-default-enable AC-
FS(cont-plcy-config)# end
```

2: Delete all IM rules in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# im-rule delete-all
AC-FS(cont-plcy-config)# end
```

3: Exchange the priority of IM access control rule 10 and rule 20 in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# im-rule priority-swap 10 20
AC-FS(cont-plcy-config)# end
```

4: Add an MSN access audit rule to the content audit policy group policyA, which allows users to conduct MSN chat, and needs to audit the user's specific account accountA or specific chat keyword keyA information.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# im-rule 2 time-range any action permit audit comment PermitUserAMSN
AC-FS(cont-plcy-config)# im-rule 2 im-type msn relation or  account accountA message keyA
AC-FS(cont-plcy-config)# end
```

【Verification】 Use the show running-config command to view the configuration status.

【Prompt Information】 1: If the configured rule-id already exists, a prompt will be given.

```
AC-FS(config)# im-rule 2 time-range any action permit audit comment PermitUserAMSN
Rule 2 already exists, please delete it first
```

2: If the public part of the rule is not configured, and the further Description of the rule is directly configured, a prompt will be given.

```
AC-FS(config)# im-rule 2 im-type msn relation or account accountA message keyA
Rule 2 is not exist
```

【Common Mistake】 -

【Platform Description】 -

6.15keyword

Add keywords to content objects.

keyword string

Delete keywords.

no keyword string

【Parameter Description】

Parameter	Description
string	The keyword that the content object contains. The maximum length is 100 bytes.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Content object configuration mode

【Default Level】 14

【Usage Guide】 Use this command to configure the keywords contained in the content object.

【Configuration Example]】1: Configure a content object objA containing the keyword hello.

```
AC-FS#  configure  terminal AC-FS(config)#
content-object objA AC-FS(content-obj-
config)# keyword hello
AC-FS(content-obj-config)# end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.16mail-rule

Enable MAIL default auditing.

mail-rule audit-default-enable

Disable the default audit function of MAIL.

no mail-rule audit-default-enable

Delete all MAIL rules under the policy group.

mail-rule delete-all

Exchange the priority of MAIL access control rules.

mail-rule priority-swap rule-id1 rule-id2

Add the public section of the MAIL access control rule to the content audit policy group.

mail-rule rule-id time-range time-name [direction { in | out | double }] action { permit | deny } [audit] [comment comment-string]

Add a further parameter description of the MAIL access control rule to the content audit policy group, mainly the keyword matching conditions of the Description rule. This command is optional. If it is not configured, it means to audit all mail information that meets the mail-rule rule-id time-range command.

mail-rule rule-id relation { and | or } [from content-object-name1] [to content-object-name2] [subject content-object-name3] [body content-object-name4] [attachment-name content- object-name5] [mail-size { greater | greater-equal | less | less-equal } file-size]

Delete the MAIL access control rule.

no mail-rule rule-id

【Parameter Description】

Parameter	Description
rule-id1	The ID of Rule 1 for the priority level to be exchanged.
rule-id2	The ID of Rule 2 for the priority level to be exchanged.
rule-id	ID identification of the rule, value range (1~200), and rule capacity of 200.
time-name	Time object name that represents the rule effective time period.
comment-string	Description of the rule.
content-object-name1	From the sender keyword, the missing item means that it is not required to match it.
content-object-name2	Recipient keyword, missing item does not match.
content-object-name3	Message title keyword, the missing item indicates that the item is not matched.
content-object-name4	Message content keyword, the missing item means that the item is not matched.
content-object-name5	Attachment name keyword, missing item indicates that the item does not match.
file-size	The File size value, which is an integer, is measured in Kbytes.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Content audit policy group configuration mode

【Default Level】 14

【Usage Guide】1: The rule-id of a rule is not allowed to be repeated in the same content audit policy group, but is allowed to be repeated in different content audit policy groups.

2: The access control rules in a content audit policy group have corresponding priorities, and the rule assigned last has the highest priority.

3: The time-name and content-object-name associated with the rule may not exist, and the rule will not take effect at this time.

4: When the rule is configured as blocking, only the or relation in relation will be valid.

5: The swap priority command is used to swap the priorities of two access control rules. After running this command, you can see that the order of the two rules has changed in show running-config, but the order of the two rules will not appear in show running-config. Order.

6: The default audit can only be configured in the default audit group whose policy group name is _AUDIT_DEFAULT, and this command will not take effect if configured in other policy groups.

【Configuration Example]】1: Enable MAIL default auditing.

```
AC-FS# configure terminal
AC-FS(config)# content-policy _AUDIT_DEFAULT AC-FS(cont-
plcy-config)# mail-rule audit-default-enable AC-FS(cont-
plcy-config)# end
```

2: Delete all MAIL rules in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# mail-rule delete-all
AC-FS(cont-plcy-config)# end
```

3: Exchange the priority of MAIL access control rule 10 and rule 20 in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# mail-rule priority-swap 10 20
AC-FS(cont-plcy-config)# end
```

4: Add a MAIL access control rule to the content audit policy group policyA to allow all users to send emails, and audit emails whose sender matches the OBJ-F keyword, or whose subject matches the OBJ-S keyword, or whose email size is less than 20000Kb.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# mail-rule 1 time-range any action permit audit comment mail-audit-1
AC-FS(cont-plcy-config)# mail-rule 1 relation or from OBJ-F subject OBJ-S mail-size less 20000
AC-FS(cont-plcy-config)# end
```

【Verification】 Use the show running-config command to view the configuration status.

【Prompt Information】 1: If the configured rule-id already exists, a prompt will be given.

```
AC-FS(config)# mail-rule 1 time-range any action permit audit comment mail-audit-1
Rule 1 already exists, please delete it first
```

2: If the public part of the rule is not configured, and the further Description of the rule is directly configured, a prompt will be given.

```
AC-FS(config)# mail-rule 1 relation or from OBJ-F subject OBJ-S mail-size less 20000
Rule 1 is not exist
```

【Common Mistake】 -

【Platform Description】 -

6.17 Regexp

Add a URL regular expression to the URL object.

regexp url-regexp

Remove URL regular expressions.

no regexp url-regexp

Add a keyword regular expression to the content object.

regexp regexp

Remove keyword regular expressions.

no regexp regexp

【Parameter Description】

Parameter	Description

url-regexp	URL regular expression, supporting the standard regular notation.
regexp	Keyword regular expression that supports the standard regular notation.

【Default Configuration】 There is no configuration by default.

【Command Mode】URL object configuration mode, content object configuration mode

【Default Level】 14

【Usage Guide】 Use this command to configure the regular expression contained in the URL object or content object.

【Configuration Example]】1: Add a regular expression to the URL object url-objA to match URLs that contain the ieft keyword.

```
AC-FS# configure terminal AC-FS(config)#
url-object url-objA AC-FS(url-obj-
config)# regexp .*ieft.*
AC-FS(url-obj-config)# end
```

2: Configure a content object objA containing the keyword hello and the regular match.ietf.org.

```
AC-FS#  configure  terminal AC-FS(config)#
content-object objA AC-FS(content-obj-
config)# keyword hello
AC-FS(content-obj-config)# regexp .*\.ietf\.org
AC-FS(content-obj-config)# end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.18 show app-audit detail

Query the detailed information of the application control audit.

show app-audit detail [export] { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name1]

[auth-subscriber subs-name2] [app-group app-group-name] [rule-name rule-name] [ip addr] [permit | deny] order-by { time | subscriber | internal-ip | app } { asc | desc } [start-item integer1 end-item integer2]

【Parameter Description】

Parameter	Description
hours	Recent time period.
yyyy mm dd	Year/Month/Day.
hh:mm:ss	Hour/minutes/seconds.
hour1	Time period filter condition: start hour period.
hour2	Time period filter conditions: End of the hour period.
hour3	Time period filter condition: start hour period.
hour4	Time period filter conditions: End of the hour period.
intf-name	Interface name.
bridge-num	Bridge number.
subs-name1	Filter condition: static user name, exact matching.
subs-name2	Filter conditions: Certified user name, exact matching.
app-group-name	Filter criteria: Application group name.
rule-name	Filter criteria: The matched rule name.
addr	Filter conditions: IP, exact match; multiple IP are separated by ",".
integer1	Query the starting position in the result set.
integer2	The end position in the query result collection.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query or export the detailed information of application control audit.

【Configuration Example]】1: Query the application control audit details of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

```
AC-FS# show app-audit detail time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
order-by time desc start-item 1 end-item 20
=====================================================================
Time: 2013-05-03 16:45:29
subscriber: /userA
auth-subscriber: any
Ip: 192.168.211.96
App:  QQ
Rule: DenyQQ
Action: deny
......
```

【Prompt Information】 -

【Platform Description】 Products with built-in storage are supported, products without built-in storage are not supported.

6.19 show app-audit stat

Query application control audit statistics.

show app-audit stat { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name1] [auth-subscriber subs-name2] [ip addr] [app-group app-group-name] [rule-name rule- name] [permit | deny]

【Parameter Description】

Parameter	Description
hours	Recent time period.
yyyy mm dd	Year/month/date.
hh:mm:ss	Hour/minutes/seconds.
hour1	Time period filter condition: start hour period.
hour2	Time period filter conditions: End of the hour period.
hour3	Time period filter condition: start hour period.
hour4	Time period filter conditions: End of the hour period.
intf-name	Interface name.
bridge-num	Bridge number.
subs-name1	Filter condition: static user name, exact matching.
subs-name2	Filter conditions: Certified user name, exact matching.
addr	Filter conditions: IP, exact match; multiple IP are separated by ",".

app-group-name	Filter criteria: Application group name.
rule-name	Filter criteria: The matched rule name.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query the statistics of application control audit.

【Configuration Example]】1: Query the application control audit statistics of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

```
AC-FS# show app-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
50
```

【Prompt Information】-

【Platform Description】 Products with built-in storage are supported, products without built-in storage are not supported.

6.20 show content-audit http-port

Display HTTP port information.

show content-audit http-port

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to view HTTP port information.

【Configuration Example]】1: View HTTP port information.

```
AC-FS#show content-audit http-port
HTTP port information in user:       80 8080 60000
HTTP port information in kernel:  80  8080 60000
```

【Prompt Information】-

【Platform Description】 -

6.21 show content-audit https-port

Display HTTPS port information.

show content-audit https-port

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to view HTTPS port information.

【Configuration Example]】1: View HTTPS port information.

```
AC-FS#show content-audit https-port
HTTPS port information in user:     443 4430
HTTPS port information in kernel:  443  4430
```

【Prompt Information】-

【Platform Description】 -

6.22 show content-audit statistics

Displays real-time statistics for content auditing.

show content-audit statistics { brief | counts }

【Parameter Description】

Parameter	Description
brief	Display a summary of live content audit statistics, showing only the last 50 records.
stat	Displays count information for real-time statistics of the content audit, including total and blocking records.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to view the summary information or count information of real-time statistics.

【Configuration Example]】 1: View the summary information of real-time statistics.

```
AC-FS#show content-audit statistics brief
audit-totle-number:3
    id      relate-user       audit-time           action  key-type
_________  ______________  ___________________  ______  ____________________________

         3  220.181.12.101    2014-02-10 00:02:50  permit  recv-mail-title: hello
         2  113.108.16.116    2014-02-09 14:26:31  permit  recv-mail-title: forward: hello
         1  192.168.66.111    2014-02-09 14:26:08  permit  send-mail-title: forward: hello
```

2: View the counting information of real-time statistics.

```
AC-FS#show content-audit statistics counts

start-time: 2014-02-09 14:25:22

application control information:
    totle-num: 0
    block-num: 0

url reference host:
    totle-num: 0
    block-num: 0

web-search keyword:
    totle-num: 0
    block-num: 0

web-bbs post information:
    totle-num: 0
    block-num: 0

web-mail information:
    totle-num: 0
    block-num: 0
```

```
MSN information:
    totle-num: 0
    block-num: 0

QQ information:
    totle-num: 0
    block-num: 0

POP3 mail information:
    totle-num: 2
    block-num: 0

SMTP mail information:
    totle-num: 1
    block-num: 0
```

【Prompt Information】-

【Platform Description】 -

6.23 show content-audit write-db

Displays the toggle status of whether the content audit audit writes to local storage.

show content-audit write-db

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to check whether the audit information of each business of the content audit is written to the local storage switch status.

【Configuration Example]】1: View the status of the content audit service writing to local storage.

```
AC-FS#show content-audit write-db
url_write_db:           1
web_search_write_db:  1
web_bbs_write_db:       1

web_mail_write_db:       1
mail_write_db:           1
im_write_db:            1
app_control_write_db:   1
```

【Prompt Information】-

【Platform Description】 Products with built-in storage are supported, products without built-in storage are not supported.

6.24 show content-policy

Displays information about policy groups.

show content-policy [policy policy-name | stat policy-name | all-rule]

【Parameter Description】

Parameter	Description
content-policy	The command ends directly with the Parameter, showing all policy groups and all policies within the group.
policy	Displays all policy details within the specified policy group and within the group.
stat	Displays the status of the specified policy group (whether the policy group exists, id how many).
all-rule	Splays all policy groups and all policy details in the group.
policy-name	Policy Group Name. Specifies that the Parameter represents the within-group detailed policy information of the query named policy-name.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query policy group related information.

【Configuration Example]】1: View all existing policy groups and the overview of all policies in the group.

```
AC-FS#show content-policy
content-policy _TOP_PRIORITY
(active)app-rule 200 time-range any app-group Block_Group action deny audit
(active)app-rule 197 time-range any app-group Block_Group action deny audit vpn

content-policy _AUDIT_DEFAULT
(active)url-rule audit-default-enable
(active)im-rule audit-default-enable
```

2: View the details of the specified policy group and all policies in the group

```
AC-FS#show content-policy policy _AUDIT_DEFAULT
```

```
policy-type: url-rule

rule-id      :0 unit-
id   :0 url-
object :any rule-
>obj_id  :0
action          :permit
audit           :Y time-
range     :
effective  :1
comment         :default_audit

_____________________________________________

policy-type: im-rule

rule-id : 0 time-
range  :
rule-type  : msn,qq
keyword           :
action          : permit
audit           : Y
effective  : 1
comment         : default_audit
```

3: Check the status of the custom policy group (whether the policy group exists and how many ids).

```
AC-FS#show content-policy stat _AUDIT_DEFAULT
exist: yes
policy_id:1
```

4: Details of all policy groups and all policies in the group.

```
AC-FS#show content-policy all-rule
content-policy _TOP_PRIORITY
policy-type: app-rule

rule-id    : 197 unit-
id  : 2
app-name    : Block_Group app-
id          : 4294967279
action          : deny
audit           : Y
```

```
vpn             : Y
vip             : N
time-range      : any
effective       : 1
comment         :

rule-id         : 200
unit-id         : 1
app-name        : Block_Group
app-id          : 4294967279
action          : deny
audit           : Y
vpn             : N
vip             : N
time-range      : any
effective       : 1
comment         :

-------------------------------------------------------------------------------------------------------------------------------

content-policy _AUDIT_DEFAULT
policy-type: url-rule

rule-id         :0
unit-id         :0
url-object      :any
rule->obj_id  :0
action          :permit
audit           :Y time-
range      :
effective       :1
comment         :default_audit

-------------------------------------------------------------------------------------------------------------------------------
policy-type: im-rule

rule-id         : 0
time-range      :
rule-type       : msn,qq
keyword         :
action          : permit
```

```
audit           : Y
effective  : 1
comment         : default_audit

_____________________________________________
```

【Prompt Information】-

【Platform Description】 -

6.25 show content-policy-relate

Displays user and policy association information in a policy view.

show content-policy-relate policy-view [{ policy policy-name | { subscriber { subs-name1 | any } |

auth-subscriber { subs-name2 | any } | ip A.B.C.D } }]

Displays user and policy association information in a user view.

show content-policy-relate user-view { subscriber { subs-name1 | any } | auth-subscriber { subs-name2

| any } | ip A.B.C.D } [detail]

【Parameter Description】

Parameter	Description
policy-name	Policy name.
subs-name1	Static user name or custom user group name.
subs-name2	Certified username.
A.B.C.D	IP address.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query the user information associated with the policy, or query the policy information associated with the user.

【Configuration Example]】1: View the association information of the static user name userA in the policy view.

```
AC-FS#show content-policy-relate policy-view subscriber userA
policy-name: policyA
disable: off
pri: 1
effective: 1 (1/1/1)
subscriber: userB userA
auth-subscriber:
```

2: View the associated information of the static user name userA in the user view.

```
AC-FS#show content-policy-relate user-view subscriber userA
policy-name: policyA
pri: 1
disable: on
effective: 1 (1/1/1)
relation-disable: on
inherit: 0
------------------------------------------------------------

policy-summary: 1/0
user-inherit: 1
```

3: View the association information of the user whose IP address is A.B.C.D in the policy view (this IP is added to the custom user group cstm_grp1).

```
AC-FS#show content-policy-relate policy-view ip A.B.C.D
policy-name: policyC
disable: off
pri: 3
effective: 1 (1/1/1)
subscriber: cstm_grp1
auth-subscriber:
```

4: View the associated information of the user whose IP address is A.B.C.D in the user view.

```
AC-FS#show content-policy-relate policy-view ip A.B.C.D
policy-name: policyC
disable: off
pri: 3
effective: 1 (1/1/1)
subscriber: cstm_grp1
auth-subscriber:
```

【Prompt Information】-

【Platform Description】 -

6.26show https-audit enable

Query the status of the HTTPS audit enable switch.

show https-audit enable

【Parameter Description】-

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query the status of the HTTPS audit enable switch.

【Configuration Example]】1: Query the status of the HTTPS audit enable switch.

```
AC-FS#show https-audit enable
{
    "code": 0,
    "msg": "",
    "data": {
        "enable": "on"
    }
}
```

【Prompt Information】-

【Platform Description】 -

6.27 show im-audit detail

Query the detailed information of IM audit.

show im-audit detail [export] { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name1] [auth-subscriber subs-name2] [direction { in | out | double }] [type { qq | msn }] [message keyword] [account account-string] [rule-name rule-name] [ip addr] [permit | deny] order-by { time | subscriber | auth-subscriber | internal-ip | direction } { asc | desc }

[start-item integer1 end-item integer2]

【Parameter Description】

Parameter	Description
hours	Recent time period.
yyyy mm dd	Year/month/date.
hh:mm:ss	Hour/minutes/seconds.
hour1	Time period filter condition: start hour period.
hour2	Time period filter conditions: End of the hour period.
hour3	Time period filter condition: start hour period.
hour4	Time period filter conditions: End of the hour period.
intf-name	Interface name.
bridge-num	Bridge number.
subs-name1	Filter condition: static user name, exact matching.
subs-name2	Filter conditions: Certified user name, exact matching.
keyword	Filter conditions: chat record.
account-string	Filter conditions: chat account.
rule-name	Filter criteria: The matched rule name.
addr	Filter conditions: IP, exact match; multiple IP are separated by ",".
integer1	Query the starting position in the result set.
integer2	The end position in the query result collection.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query or export the detailed information of IM audit.

【Configuration Example]】1: Query the MSN audit details of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

```
AC-FS# show im-audit detail time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
type msn order-by time desc start-item 1 end-item 20
================================================================================================
Time: 2013-05-03 15:45:59
App-type: msn
Sender: userA@hotmail.com
Receiver: userB@yahoo.com
Direction: out
Path: GigabitEthernet 0/5
Ip: 192.168.211.96
User: /userA Auth-
User: Match-Rule:
ruleA Action:
permit Message:
hello!
.....
```

【Prompt Information】 -

【Platform Description】 Products with built-in storage are supported, products without built-in storage are not supported.

6.28 show im-audit stat

Query the statistics of IM auditing.

show im-audit stat { recent hours | time-range from yyyy mm dd hh:mm::ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name1] [auth-subscriber subs-name2] [direction { in | out | double }] [type { qq | msn }] [message keyword] [account account-string] [rule-name rule-name] [ip addr] [permit | deny]

【Parameter Description】

Parameter	Description
hours	Recent time period.
yyyy mm dd	Year/month/date.
hh:mm:ss	Hour/minutes/seconds.
hour1	Time period filter condition: start hour period.
hour2	Time period filter conditions: End of the hour period.
hour3	Time period filter condition: start hour period.
hour4	Time period filter conditions: End of the hour period.

intf-name	Interface name.
bridge-num	Bridge number.
subs-name1	Filter condition: static user name, exact matching.
subs-name2	Filter conditions: Certified user name, exact matching.
keyword	Filter conditions: chat record.
account-string	Filter conditions: chat account.
rule-name	Filter criteria: The matched rule name.
addr	Filter conditions: Intranet ip.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query the statistics of IM audit.

【Configuration Example]】1: Query the MSN audit statistics of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

```
AC-FS# show im-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA type
msn
50
```

【Prompt Information】-

【Platform Description】 Products with built-in storage are supported, products without built-in storage are not supported.

6.29 show mail-audit attachment-info

Query the attachment information of an email.

show mail-audit attachment-info timestamp timestamp rand-id rand-id

【Parameter Description】

Parameter	Description
timestamp	time stamp
rand-id	random id

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 First use the command show mail-audit detail to view the timestamp and random id of the email, and then use this command to query the attachment information of a certain email.

【Configuration Example]】1: Query the attachment information of the email whose timestamp is 1286849291 and rand-id is 1087821567.

```
AC-FS#show mail-audit attachment-info timestamp 1286849291 rand-id 1087821567
Size(Byte)  Path
============================================================
80646    mnt/sata/mail/20130503/unknown(09-01-19-44-40).gif
150528       mnt/sata/mail/20130503/test-file.doc
```

【Prompt Information】-

【Platform Description】 -

6.30show mail-audit detail

Query the detailed information of the MAIL audit.

show mail-audit detail [export] { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name1] [auth-subscriber subs-name2] [ip addr] [direction { in | out | double }] [from keyword1] [to keyword2] [subject keyword3] [rule-name rule-name] [permit | deny] order-by { time | subscriber | auth-subscriber | internal-ip | direction | send-mail-addr | mail-size } { asc | desc } [start-item integer1 end-item integer2]

【Parameter Description】

Parameter	Description
hours	Recent time period.
yyyy mm dd	Year/month/date.
hh:mm:ss	Hour/minutes/seconds.
hour1	Time period filter condition: start hour period.
hour2	Time period filter conditions: End of the hour period.
hour3	Time period filter condition: start hour period.
hour4	Time period filter conditions: End of the hour period.
intf-name	Interface name.
bridge-num	Bridge number.

subs-name1	Filter condition: static user name, exact matching.
subs-name2	Filter conditions: Certified user name, exact matching.
addr	Filter conditions: IP, exact match; multiple IP are separated by ",".
keyword1	Filter criteria: Message sender keyword.
keyword2	Filter criteria: Message Receiver keyword.
keyword3	Filter criteria: Message subject keyword.
rule-name	Filter criteria: The matched rule name.
integer1	Query the starting position in the result set.
integer2	The end position in the query result collection.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query or export the detailed information of MAIL audit.

【Configuration Example]】1: Query the MAIL audit details of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

```
AC-FS# show mail-audit detail time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
order-by time desc start-item 1 end-item 20
=============================================================================================
Time: 2013-05-03 15:45:59
App-type: SMTP
Direction: out
Path: GigabitEthernet 0/5
Ip: 192.168.211.96
User: /userA Auth-
User: Match-Rule:
ruleA
Action: permit
```

```
Timestamp: 1287027112
Rand-id: 1686175891
From: userA@hotmail.com
To: userB@yahoo.com
Subject: hello
Body: hello
......
```

【Prompt Information】-

【Platform Description】 -

6.31 show mail-audit stat

Query the statistics of MAIL audit.

show mail-audit stat { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name1] [auth-subscriber subs-name2] [ip addr] [direction { in | out | double }] [from keyword1] [to keyword2] [subject keyword3] [rule-name rule-name] [permit | deny]

【Parameter Description】

Parameter	Description
hours	Recent time period.
yyyy mm dd	Year/month/date.
hh:mm:ss	Hour/minutes/seconds.
hour1	Time period filter condition: start hour period.
hour2	Time period filter conditions: End of the hour period.
hour3	Time period filter condition: start hour period.
hour4	Time period filter conditions: End of the hour period.
intf-name	Interface name.
bridge-num	Bridge number.
subs-name1	Filter condition: static user name, exact matching.
subs-name2	Filter conditions: Certified user name, exact matching.
addr	Filter conditions: IP, exact match; multiple IP are separated by ",".
keyword1	Filter criteria: Message sender keyword.
keyword2	Filter criteria: Message Receiver keyword.
keyword3	Filter criteria: Message subject keyword.
rule-name	Filter criteria: The matched rule name.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query the statistics of MAIL audit.

【Configuration Example]】1: Query the MAIL audit statistics of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

```
AC-FS# show mail-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
50
```

【Prompt Information】-

【Platform Description】 -

6.32 show url-audit detail

Query URL audit details.

show url-audit detail [export] { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name] [auth-subscriber auth-subs-name] [ip addr] [url-class class-name | url-object obj-name | url url-string | url-host host-string1] [host host-string2] [permit | deny] [order-by time | url-class | url | host | ip] { asc | desc } [start -item integer1 end-item integer2]

【Parameter Description】

Parameter	Description
hours	Recent time period.
yyyy mm dd	Year/month/date.
hh:mm:ss	Hour/minutes/seconds.
hour1	Time period filter condition: start hour period.
hour2	Time period filter conditions: End of the hour period.
hour3	Time period filter condition: start hour period.
hour4	Time period filter conditions: End of the hour period.
intf-name	Interface name.
bridge-num	Bridge number.
subs-name1	Filter condition: static user name, exact matching.
subs-name2	Filter conditions: Certified user name, exact matching.
addr	Filter conditions: IP, exact match; multiple IP are separated by ",".
class-name	Filter condition: URL classification name, exact matching.
obj-name	Filter condition: URL object name, exact match.
url-string	Filter conditions: URL, string, fuzzy matching.
host-string1	Filter conditions: HOST string, exact matching.
host-string2	Filter conditions: HOST site, exact match.

integer1	Query the starting position in the result set.
integer2	The end position in the query result collection.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query or export the detailed information of URL auditing.

【Configuration Example]】1: Query the URL audit details of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

```
AC-FS# show url-audit detail time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
order-by time desc start-item 1 end-item 20
=============================================================================================
Time: 2013-05-03 15:45:59
Ip: 192.168.211.96
Subscriber: /userA
Auth-subscriber:
Match-rule: ruleA
Action: permit
URL: http://www.ietf.org/
URL-class: Foreign
websites
```

【Prompt Information】-

【Platform Description】 -

6.33 show url-audit stat

Query URL auditing statistics.

show url-audit stat { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name] [auth-subscriber auth-subs-name] [ip addr] [url-class class-name | url-object obj-name] [host host-string] [permit | deny]

【Parameter Description】

Parameter	Description
hours	Recent time period.

yyyy mm dd	Year/month/date.
hh:mm:ss	Hour/minutes/seconds.
hour1	Time period filter condition: start hour period.
hour2	Time period filter conditions: End of the hour period.
hour3	Time period filter condition: start hour period.
hour4	Time period filter conditions: End of the hour period.
intf-name	Interface name.
bridge-num	Bridge number.
subs-name1	Filter condition: static user name, exact matching.
subs-name2	Filter conditions: Certified user name, exact matching.
addr	Filter conditions: IP, exact match; multiple IP are separated by ",".
class-name	Filter condition: URL classification name, exact matching.
obj-name	Filter condition: URL object name, exact match.
host-string	Filter conditions: HOST site, exact match.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query the statistics of URL auditing.

【Configuration Example]】1: Query the URL audit statistics of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

```
AC-FS# show url-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
500
```

【Prompt Information】-

【Platform Description】 -

6.34 show url-audit top

Query URL site access ranking TOPN.

show url-audit top n [export] { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name] [auth-subscriber auth-subs-name] [url-class class-name | url-object obj-name] [host host-string] [permit | deny] [order-by time |

url-class | url | url-class | host-times]

【Parameter Description】

Parameter	Description
n	Number of Top n's (1~100).
hours	Recent time period.
yyyy mm dd	Year/month/date.
hh:mm:ss	Hour/minutes/seconds.
hour1	Time period filter condition: start hour period.
hour2	Time period filter conditions: End of the hour period.
hour3	Time period filter condition: start hour period.
hour4	Time period filter conditions: End of the hour period.
intf-name	Interface name.
bridge-num	Bridge number.
subs-name1	Filter condition: static user name, exact matching.
subs-name2	Filter conditions: Certified user name, exact matching.
addr	Filter conditions: IP, exact match; multiple IP are separated by ",".
class-name	Filter condition: URL classification name, exact matching.
obj-name	Filter condition: URL object name, exact match.
host-string	Filter conditions: HOST site, exact match.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query or export URL site access ranking TOPN.

【Configuration Example]】1: Query the TOP2 site access ranking within 24 hours

```
AC-FS# show url-audit top 2 recent 24
HOST                          Times url-class     url-object
============================================================
www.ietf.org                                  class1          obj1
32349
www.w3c.org                                   class2          obj2
30032
```

【Prompt Information】-

【Platform Description】 -

6.35 show url-class system

Displays the category names of the current URL library of the system.

show url-class system [class { id class-id | name class-name }]

Displays the description information of the current URL library of the system.

show url-class system comment [class { id class-id | name class-name }]

Displays current custom modification information for the system URL library.

show url-class system custom [class { id class-id | name class-name }]

Displays information about the precise filter library.

show url-class system exact

【Parameter Description】

Parameter	Description
class-name	View the information of the specified system classification name class-name; if no class is specified, it means to view all systems URL classification information.
class-id	View the information for the specified system classification ID class-id..

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query information about the system URL library.

【Configuration Example]】1: View the category names of the current URL library of the system.

```
AC-FS# show url-class system version-1.0
2010-4-22
system-url-class-number:32
Category 1          Job recruitment
                        IT class
                        WEB communication
                    violence
          virus

Category 2          science
                        Adult
                    (omitted below)
```

2: View the current URL library grouping and classification information of the system.

```
AC-FS# show url-class system custom
version-1.0
2010-4-22
system-url-class-number:32
```

```
consumption-amount:2
remain-amount:998 （These lines are some necessary statistical information）

  url-class: Job recruitment
          comment: Job recruitment
          Description
            add: add1.com
            add: add2.com
           move: move1.com
    url-class:  military affairs
                                  com
    ment: Military classDescription
          comment: IT  category
          Description
            add: add1.com
            add: add2.com
           move: move1.com
Category 2
    url-class:
          comment:
    (omitted below)
```

3: View the current URL library classification and Description information of the system.

```
AC-FS# show url-class system comment version-1.0
2010-4-22
System url class number:32
category 1
                    Job recruitment : Description information 1
                    IT class : Descriptioninformation 2
                    WEB communication : Descriptioninformation 3
……（The following slightly）
```

4: View the relevant information of the precise filter library.

```
AC-FS# show url-class system exact
exact-filter: disable
```

【Prompt Information】-

【Platform Description】 -

6.36 show url-class url

Displays the system url category to which the specified url-string belongs and the actual url category under the current configuration.

show url-class url url-string

【Parameter Description】

Parameter	Description
url-string	String representing the url.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query the system url category to which the specified url-string belongs and the actual url category under the current configuration.

【Configuration Example]】1: Display the category information whose URL is AC-FS.com.cn.

```
AC-FS# show url-class url AC-FS.com.cn url:AC-FS.com.cn
default-system-class: commerce
modified-system-class:
custom-class:test1
```

【Prompt Information】-

【Platform Description】 -

6.37 show url-class user-cfg

Displays configuration information for custom URL categories.

show url-class user-cfg [class-name]

【Parameter Description】

Parameter	Description
class-name	Custom classification name.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query the configuration information of the custom URL category.

【Configuration Example]】1: Display the configuration information of each custom URL category.

```
AC-FS# show url-class user-cfg
url-class:CLASSA
url:ietf.org
comment:comment for CLASSA
url-class:CLASSB
url:w3c.org
comment:comment for CLASSB
```

2: Display the configuration information of the specified URL category.

```
AC-FS# show url-class user-cfg CLASSA
url-class:CLASSA
url:ietf.org
comment:comment for CLASSA
```

【Prompt Information】-

【Platform Description】 -

6.38 show vid-audit detail

Query the detailed information of virtual identity audit.

show vid-audit detail [export] { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [subscriber subs-name1] [auth-subscriber subs-name2] [type { weibo | weixin }] [uid uid-string] [nickname nick-string] [ip addr1] [mac addr2] order-by { time | subscriber | auth-subscriber | internal-ip | uid | mac } { asc | desc } [start-item integer1 end-item integer2]

【Parameter Description】

Parameter	Description
hours	Recent time period.
yyyy mm dd	Year/month/date.
hh:mm:ss	Hour/minutes/seconds.
hour1	Time period filter condition: start hour period.
hour2	Time period filter conditions: End of the hour period.
hour3	Time period filter condition: start hour period.
hour4	Time period filter conditions: End of the hour period.
subs-name1	Filter condition: static user name, exact matching.
subs-name2	Filter conditions: Certified user name, exact matching.
uid-string	Filter conditions: account number UID.
nick-string	Filter conditions: account nickname.
addr1	Filter conditions: IP, exact match; multiple IP are separated by ",".
addr2	Filter condition: MAC address, exact match; multiple addresses are separated by ",".
integer1	Query the starting position in the result set.
integer2	The end position in the query result collection.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query or export the detailed information of virtual identity audit.

【Configuration Example]】1: Query the virtual identity audit details of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

```
AC-FS# show vid-audit detail time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
type msn order-by time desc start-item 1 end-item 20
=============================================================================================
day_time: 2013-05-03 15:45:59
internal_ip: 192.168.211.96
mac_addr: 00d0.1234.abcd
usr_grp: /
usr_name: /userA
vid_type: wechat
vid_action: LOGOUT
uid: 1755006665
nick_name:
......
```

【Prompt Information】-

【Platform Description】 -

6.39 show vid-audit stat

Query statistics for virtual identity auditing.

show vid-audit stat { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [subscriber subs-name1] [auth-subscriber subs-name2] [type { weibo | weixin }] [uid uid-string] [nickname nick-string] [ip addr1] [mac addr2]

【Parameter Description】

Parameter	Description
hours	Recent time period.
yyyy mm dd	Year/month/date.
hh:mm:ss	Hour/minutes/seconds.
hour1	Time period filter condition: start hour period.

hour2	Time period filter conditions: End of the hour period.
hour3	Time period filter condition: start hour period.
hour4	Time period filter conditions: End of the hour period.
subs-name1	Filter condition: static user name, exact matching.
subs-name2	Filter conditions: Certified user name, exact matching.
uid-string	Filter conditions: account number UID.
nick-string	Filter conditions: account nickname.
addr1	Filter conditions: IP, exact match; multiple IP are separated by ",".
addr2	Filter condition: MAC address, exact match; multiple addresses are separated by ",".

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query the statistics of virtual identity audit.

【Configuration Example]】1: Query the MSN audit statistics of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

```
AC-FS# show vid-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
type msn
50
```

【Prompt Information】-

【Platform Description】 -

6.40 show web-bbs-audit detail

Query the detailed information of WEB-BBS audit.

show web-bbs-audit detail [export] { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name1] [auth-subscriber subs-name2] [ip addr] [content keyword] [rule-name rule-name] [permit | deny] order-by { time | subscriber | auth-subscriber | internal-ip | url } { asc | desc } [start-item integer1 end-item integer2]

【Parameter Description】

Parameter	Description
hours	Recent time period.
yyyy mm dd	Year/month/date.
hh:mm:ss	Hour/minutes/seconds.
hour1	Time period filter condition: start hour period.
hour2	Time period filter conditions: End of the hour period.
hour3	Time period filter condition: start hour period.
hour4	Time period filter conditions: End of the hour period.
intf-name	Interface name.
bridge-num	Bridge number.
subs-name1	Filter condition: static user name, exact matching.
subs-name2	Filter conditions: Certified user name, exact matching.
addr	Filter conditions: IP, exact match; multiple IP are separated by ",".
keyword	Filter conditions: filter keywords, support multi-keyword filtering, and separate keywords with commas.
rule-name	Filtering condition: Matching rule name, support multiple rule name filtering, different rule names are separated by half-width commas.
integer1	Query the starting position in the result set.
integer2	The end position in the query result collection.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query or export the detailed information of WEB-BBS audit.

【Configuration Example]】1: Query the WEB-BBS audit details of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

```
AC-FS# show web-bbs-audit detail time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber
userA order-by time desc start-item 1 end-item 20
=========================================================================
Time: 2013-05-03 16:45:29
subscriber: /userA
auth-subscriber: any
Ip: 192.168.211.96
Rule: ruleA
Action: permit
Title: hello
Body: hello
......
```

【Prompt Information】-

【Platform Description】 -

6.41 show web-bbs-audit stat

Query WEB-BBS audit statistics.

show web-bbs-audit stat { recent hours | time-range from yyyy mm dd hh:mm::ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name1] [auth-subscriber subs-name2] [ip addr] [content keyword] [rule-name rule-name] [permit | deny]

【Parameter Description】

Parameter	Description
hours	Recent time period.
yyyy mm dd	Year/month/date.
hh:mm:ss	Hour/minutes/seconds.
hour1	Time period filter condition: start hour period.
hour2	Time period filter conditions: End of the hour period.
hour3	Time period filter condition: start hour period.
hour4	Time period filter conditions: End of the hour period.
intf-name	Interface name.
bridge-num	Bridge number.
subs-name1	Filter condition: static user name, exact matching.
subs-name2	Filter conditions: Certified user name, exact matching.

addr	Filter conditions: IP, exact match; multiple IP are separated by ",".
keyword	Filter conditions: filter keywords, support multi-keyword filtering, and separate keywords with commas.
rule-name	Filtering condition: Matching rule name, support multiple rule name filtering, different rule names are separated by half-width commas.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query the WEB-BBS audit statistics.

【Configuration Example]】1: Query the WEB-BBS audit statistics of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

```
AC-FS# show web-bbs-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
50
```

【Prompt Information】-

【Platform Description】 -

6.42 show web-mail-audit attachment-info

Query the attachment information of an email.

show web-mail-audit attachment-info timestamp timestamp rand-id rand-id

【Parameter Description】

Parameter	Description
timestamp	Time stamp.
rand-id	Stochastic id.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 First use the command show web-mail-audit detail to view the timestamp and random id of the email, and then use this

command to query the attachment information of a certain email.

【Configuration Example]】1: Query the attachment information of the email whose timestamp is 1286849291 and rand-id is 1087821567.

```
AC-FS#show web-mail-audit attachment-info timestamp 1286849291 rand-id 1087821567
Size(Byte)  Path
================================================================
80646     mnt/sata/mail/20130503/unknown(09-01-19-44-40).gif
150528       mnt/sata/mail/20130503/test-file.doc
```

【Prompt Information】-

【Platform Description】 -

6.43 show web-mail-audit detail

Query the detailed information of the WEB-MAIL audit.

show web-mail-audit detail [export] { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name1] [auth-subscriber subs-name2] [ip addr] [direction { in | out | double }] [from keyword1] [to keyword2] [subject keyword3] [rule-name

rule-name] [permit | deny] order-by { time | subscriber | auth-subscriber | internal-ip | direction |

send-mail-addr } { asc | desc } [start-item integer1 end-item integer2]

【Parameter Description】

Parameter	Description
hours	Recent time period.
yyyy mm dd	Year/month/date.
hh:mm:ss	Hour/minutes/seconds.
hour1	Time period filter condition: start hour period.
hour2	Time period filter conditions: End of the hour period.
hour3	Time period filter condition: start hour period.
hour4	Time period filter conditions: End of the hour period.
intf-name	Interface name.
bridge-num	Bridge number.
subs-name1	Filter condition: static user name, exact matching.

subs-name2	Filter conditions: Certified user name, exact matching.
addr	Filter conditions: IP, exact match; multiple IP are separated by ",".
keyword1	Filter criteria: Message sender keyword.
keyword2	Filter criteria: Message Receiver keyword.
keyword3	Filter criteria: Message subject keyword.
rule-name	Filter criteria: The matched rule name.
integer1	Query the starting position in the result set.
integer2	The end position in the query result collection.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query or export the detailed information of WEB-MAIL audit.

【Configuration Example]】1: Query the WEB-MAIL audit details of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

```
AC-FS# show web-mail-audit detail time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber
userA order-by time desc start-item 1 end-item 20
==============================================================================================
Time: 2013-05-03 15:45:59
Direction: out
Path: GigabitEthernet 0/5
Ip: 192.168.211.96
User: /userA Auth-
User: Match-Rule:
ruleA
Action: permit
```

```
Timestamp: 1287027112
Rand-id: 1686175891
From: userA@hotmail.com
To: userB@yahoo.com
Subject: hello
Body: hello
......
```

【Prompt Information】-

【Platform Description】 -

6.44 show web-mail-audit stat

Query the statistics of the WEB-MAIL audit.

show web-mail-audit stat { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name1] [auth-subscriber subs-name2] [ip addr] [direction { in | out | double }] [from keyword1] [to keyword2] [subject keyword3] [rule-name rule-name] [permit | deny]

【Parameter Description】

Parameter	Description
hours	Recent time period.
yyyy mm dd	Year/month/date.
hh:mm:ss	Hour/minutes/seconds.
hour1	Time period filter condition: start hour period.
hour2	Time period filter conditions: End of the hour period.
hour3	Time period filter condition: start hour period.
hour4	Time period filter conditions: End of the hour period.
intf-name	Interface name.
bridge-num	Bridge number.
subs-name1	Filter condition: static user name, exact matching.
subs-name2	Filter conditions: Certified user name, exact matching.
addr	Filter conditions: IP, exact match; multiple IP are separated by ",".
keyword1	Filter criteria: Message sender keyword.
keyword2	Filter criteria: Message Receiver keyword.
keyword3	Filter criteria: Message subject keyword.
rule-name	Filter criteria: The matched rule name.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query the WEB-MAIL audit statistics.

【Configuration Example]】1: Query the WEB-MAIL audit statistics of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

```
AC-FS# show web-mail-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
50
```

【Prompt Information】-

【Platform Description】 -

6.45 show web-search-audit detail

Query the detailed information of the WEB-SEARCH audit.

show web-search-audit detail [export] { recent hours | time-range from yyyy mm dd hh:mm:ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name1] [auth-subscriber subs-name2] [ip addr] [keyword keyword] [rule-name rule-name] [permit | deny] order-by { time | subscriber | auth-subscriber | internal-ip | url } { asc | desc } [start-item integer1 end-item integer2]

【Parameter Description】

Parameter	Description
hours	Recent time period.
yyyy mm dd	Year/month/date.
hh:mm:ss	Hour/minutes/seconds.
hour1	Time period filter condition: start hour period.
hour2	Time period filter conditions: End of the hour period.
hour3	Time period filter condition: start hour period.
hour4	Time period filter conditions: End of the hour period.
intf-name	Interface name.
bridge-num	Bridge number.
subs-name1	Filter condition: static user name, exact matching.
subs-name2	Filter conditions: Certified user name, exact matching.
addr	Filter conditions: IP, exact match; multiple IP are separated by ",".
keyword	Filter conditions: filter keywords, support multi-keyword filtering, and separate keywords with commas.
rule-name	Filtering condition: Matching rule name, support multiple rule name filtering, different rule names are separated by half-width commas.
integer1	Query the starting position in the result set.

integer2	The end position in the query result collection.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query or export the detailed information of WEB-SEARCH audit.

【Configuration Example]】1: Query the WEB-SEARCH audit details of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

```
AC-FS# show web-search-audit detail time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber
userA order-by time desc start-item 1 end-item 20
==========================================================================
Time: 2013-05-03 16:45:29
subscriber: /userA
auth-subscriber: any
Ip: 192.168.211.96
Rule: ruleA
Action: permit
URL: http://www.baidu.com/s?ie=utf-8&bs=hello&rsv_bp=1&rsv_spt=3&wd=hello
search-word: hello
......
```

【Prompt Information】-

【Platform Description】 -

6.46 show web-search-audit stat

Query WEB-SEARCH audit statistics.

show web-bbs-audit stat { recent hours | time-range from yyyy mm dd hh:mm::ss to yyyy mm dd hh:mm:ss | day-interval yyyy mm dd to yyyy mm dd [hour-interval hour1 to hour2 [hour3 to hour4]] } [interface intf-name | bridge bridge-num] [subscriber subs-name1] [auth-subscriber subs-name2] [ip addr] [keyword keyword] [rule-name rule-name] [permit | deny]

【Parameter Description】

Parameter	Description
hours	Recent time period.
yyyy mm dd	Year/month/date.

hh:mm:ss	Hour/minutes/seconds.
hour1	Time period filter condition: start hour period.
hour2	Time period filter conditions: End of the hour period.
hour3	Time period filter condition: start hour period.
hour4	Time period filter conditions: End of the hour period.
intf-name	Interface name.
bridge-num	Bridge number.
subs-name1	Filter condition: static user name, exact matching.
subs-name2	Filter conditions: Certified user name, exact matching.
addr	Filter conditions: IP, exact match; multiple IP are separated by ",".
keyword	Filter conditions: filter keywords, support multi-keyword filtering, and separate keywords with commas.
rule-name	Filtering condition: Matching rule name, support multiple rule name filtering, different rule names are separated by half-width commas.

【Command Mode】 Privileged mode

【Default Level】 14

【Usage Guide】 Use this command to query the statistical information of WEB-SEARCH audit.

【Configuration Example]】1: Query the WEB-SEARCH audit statistics of user userA from 0:00 on 2013-5-1 to 24:00 on 2013-5-7.

```
AC-FS# show web-search-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber
userA
50
```

【Prompt Information】-

【Platform Description】 -

6.47url

Add URL entries to the URL category.

url url-string

Delete the URL entry.

no url url-string

【Parameter Description】

Parameter	Description
url-string	URL entries included in the URL classification, supporting pattern matching:
	1.If the URL contained in the custom Web site classification is a subdirectory under the domain name, then match all the files under that subdirectory. For example, the URL is ietf.org/2006 and matches all the contents in the ietf.org/2006 directory. 2. If the URL contained in the custom website category is a domain name and does not contain a path, it will match all accesses to the domain name and its subdomains. For example, if the URL is "ietf.org", it will match to "www.ieft.org" ″ and access to subdomains such as "download.ietf.org" and "news.ietf.org".

【Default Configuration】 There is no configuration by default.

【Command Mode】 URL classification configuration mode

【Default Level】 14

【 Usage Guide 】 1: URL pattern matching currently only supports level 2 directories, and users are not allowed to configure "ietf.org/2006/12/1";

2: URL subdomain pattern matching currently only supports level 4 subdomains. If the user configuration is "test.rfc.download.ietf.org", it can only match exact domain names.

【Configuration Example]】 1: Add an entry for the URL classification classA: ietf.org.

```
AC-FS# configure terminal AC-
FS(config)# url-class classA AC-
FS(url-cls-config)# url ietf.org
AC-FS(url-cls-config)#end
```

【Verification】 Use the show running-config command to view the configuration status.

【Prompt Information】 1: If the configured URL format is incorrect, a prompt will be given.

```
AC-FS(config)# url ietf.org/2006/12/1
Format error
```

【Common Mistake】-

【Platform Description】 -

6.48 url-audit

Enable the corresponding URL optimization audit function.

url-audit { exact-filter | except-postfix | except-regexp [regexp] | only-get | optimize-cache [time] }

Turn off the corresponding URL optimization audit function.

no url-audit { exact-filter | except-postfix | except-regexp [regexp] | only-get | optimize-cache [time] }

【Parameter Description】

Parameter	Description
regexp	The Parameter is a regular expression and the URL matching the feature is not be audited.
time	The Parameter is run in seconds, without repeating the time time audit of the same URL and the link page opened from the URL web page.

【Default Configuration】 It is enabled by default, and the command is not displayed. Commands are displayed only after the no command has been executed.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 1: If no regular expression is specified when url-audit except-regexp is enabled, it will be specified as ".*=.*&.*=.*" by default.

2: When url-audit except-postfix is enabled, the following URLs with suffixes, jpg, css, js, gif, png, swf, bmp, ico, ng, dll, GIF, JPG, xml, ini, will not be audited.

3: Enable url-audit optimize-cache, the default time is 30s.

【Configuration Example]】1: Enable only audit HTTP GET.

```
AC-FS# configure terminal AC-
FS(config)# url-audit only-get
AC-FS(config)#end
```

2: Configure the URL access that matches the default regular expression (.*=.*&.*=.*) to not be audited.

```
AC-FS# configure terminal AC-FS(config)#
url-audit except-regexp
AC-FS(config)# end
```

3: URL access with suffixes such as configuration pictures is not audited.

```
AC-FS# configure terminal
AC-FS(config)# url-audit except-postfix AC-
FS(config)# end
```

4: Within the specified 60s, the duplicate URL access of the same IP will not be audited and the links clicked from the URL page will not be audited.

```
AC-FS# configure terminal
AC-FS(config)# url-audit optimize-cache 60 AC-
FS(config)# end
```

【Verification】 Use the show running-config command to view the configuration status.

【Prompt Information】 -

【Common Mistake】 -

【Platform Description】 -

6.49 url-class

Specify the URL category name and enter the URL category configuration mode.

url-class class-name

Remove URL categorization.

no url-class class-name

【Parameter Description】

Parameter	Description
class-name	The URL taxonomy name.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Use this command to configure URL classification.

【Configuration Example]】1: Add a URL category classA.

```
AC-FS# configure terminal AC-
FS(config)# url-class classA
AC-FS(url-obj-config)#end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.50 url-filter-notice

Configure the content displayed on the URL filtering prompt page.

url-filter-notice display [text]

Disable the URL filtering prompt page display function.

no url-filter-notice

【Parameter Description】

Parameter	Description
text	The URL filters the information displayed on the prompt page. Do not enter the display default information.

【Default Configuration】 Open by default. The default display content is:

"You are forbidden to visit the website, please contact webmaster!"

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Use this command to configure the content displayed on the URL filtering prompt page.

【Configuration Example]】1: Configure the information displayed on the URL filtering prompt page:

```
AC-FS# configure terminal
AC-FS(config)# url-filter-notice display The web site you visit has been banned, please contact your administrator!
AC-FS(config)#end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.51 url-object

Specify the URL object name and enter URL object configuration mode.

url-object object-name

Delete the URL object.

no url-object object -name

【Parameter Description】

Parameter	Description
object-name	The URL object name. The maximum length is 40 bytes.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Global mode

【Default Level】 14

【Usage Guide】 Use this command to configure the URL object. The URL object capacity is 100.

【Configuration Example]】1: Add a URL object objA.

```
AC-FS# configure terminal AC-
FS(config)# url-object objA
AC-FS(url-obj-config)# end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.52 url-redirect-rule

Delete all URL redirection rules under the policy group.

url-redirect-rule delete-all

Exchange the priority of URL redirection access control rules.

url-redirect-rule priority-swap rule-id1 rule-id2

Add URL redirection access control rules to the content audit policy group.

url-redirect-rule rule-id time-range time-name from url-1 to url-2 [comment comment-string]

Remove URL redirection access control rules.

no url-redirect-rule rule-id

【Parameter Description】

Parameter	Description
rule-id1	The ID of Rule 1 for the priority level to be exchanged.
rule-id2	The ID of Rule 2 for the priority level to be exchanged.
rule-id	ID identification of the rule, the value range (1~200), and a rule capacity of 200.
time-name	Time object name that represents the rule effective time period.
url-1	The url address required for redirection.

url-2	The url address after the redirect.
comment-string	Description of the rule.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Content audit policy group configuration mode

【Default Level】 14

【Usage Guide】 1: The rule-id of a rule is not allowed to be repeated in the same content audit policy group, but is allowed to be repeated in different content audit policy groups.

2: The URL redirection rules in a content audit policy group have corresponding priorities, and the rule assigned last has the highest priority.

3: The time-name associated with the rule may not exist, and the rule will not take effect at this time.

4: The swap priority command is used to swap the priorities of two URL redirection rules. After running this command, you can see that the order of the two rules has changed in show running-config, but show running-config will not appear. the command.

【Configuration Example]】 1: Delete all URL redirection rules in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# url-redirect-rule delete-all
AC-FS(cont-plcy-config)# end
```

2: Exchange the priority of URL redirection rule 10 and rule 20 in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# url-redirect-rule priority-swap 10 20
AC-FS(cont-plcy-config)# end
```

3: Add a URL redirection rule for the content audit policy group policyA to redirect www.sina.com.cn to www.AC-FS.com.cn.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# url-redirect-rule 2 time-range any from www.sina.com.cn to www.AC-
FS.com.cn comment sina-redirect
AC-FS(cont-plcy-config)# end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】1: If the configured rule-id already exists, a prompt will be given.

```
AC-FS(config)# url-redirect-rule 2 time-range any from www.sina.com.cn to www.AC-FS.com.cn comment
sina-redirect
Rule 2 already exists, please delete it first
```

【Common Mistake】-

【Platform Description】 -

6.53 url-rule

Enable URL default auditing.

url-rule audit-default-enable

Disable URL default auditing.

no url-rule audit-default-enable

Delete all URL rules under the policy group.

url-rule delete-all

Exchange the priority of URL access control rules.

url-rule priority-swap rule-id1 rule-id2

Add URL access control rules to the content audit policy group.

url-rule rule-id url-object url-obj-name time-range time-name action { permit | deny } [audit] [comment

comment-string]

Delete URL access control rules.

no url-rule rule-id

Enable the URL loose whitelist function.

url-rule apply-referer

Disable the URL loose whitelist function.

no url-rule apply-referer

【Parameter Description】

Parameter	Description
rule-id1	The ID of Rule 1 for the priority level to be exchanged.
rule-id2	The ID of Rule 2 for the priority level to be exchanged.
rule-id	ID of rule 2 whose priority is to be exchanged.
url-obj-name	The ID of the rule, the value range (1~200), and the rule capacity is 200.
time-name	the URL object associated with the rule
comment-string	The name of the time object representing the effective time period of the rule.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Content audit policy group configuration mode

【Default Level】 14

【Usage Guide】 1: The rule-id of a rule is not allowed to be repeated in the same content audit policy group, but is allowed to be repeated in different content audit policy groups.

2: The access control rules in a content audit policy group have corresponding priorities, and the rule assigned last has the highest priority.

3: The time-name and url-obj-name associated with the rule may not exist, and the rule will not take effect at this time.

4: The swap priority command is used to swap the priorities of two access control rules. After running this command, you can see that the order of the two rules has changed in show running-config, but the order of the two rules will not appear in show running-config. Order.

5: The default audit can only be configured in the default audit group named _AUDIT_DEFAULT in the policy group, and this command will not take effect if configured in other policy groups.

6: The url-rule apply-referer needs to be matched with the URL audit filtering policy. After the configuration is complete, in addition to matching the corresponding URL, the URL rule will also use the referer Field to match the rule. If you only configure this command without enabling the corresponding URL audit filtering rule, it will have no actual effect. It is mainly used in the URL whitelist policy, which can allow both websites and their sub-sites in the whitelist.

【Configuration Example]】 1: Enable URL default auditing.

```
AC-FS# configure terminal
AC-FS(config)# content-policy _AUDIT_DEFAULT AC-FS(cont-
plcy-config)# url-rule audit-default-enable AC-FS(cont-
plcy-config)# end
```

2: Delete all URL rules in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# url-rule delete-all
AC-FS(cont-plcy-config)# end
```

3: Exchange the priority of URL access control rule 10 and rule 20 in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# url-rule priority-swap 10 20
AC-FS(cont-plcy-config)# end
```

4: Add a URL access audit rule to the content audit policy group policyA, which does not allow access to the URL in the URL object url-objA, and needs to audit this type of URL access.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# url-rule 2 url-object url-objA time-range any action deny audit
AC-FS(cont-plcy-config)# end
```

5: Enable the URL loose whitelist function.

```
AC-FS# configure terminal AC-
FS(config)#url-rule apply-referer
AC-FS(config)#end
```

【Verification】 Use the show running-config command to view the configuration status.

【Prompt Information】 1: If the configured rule-id already exists, a prompt will be given.

```
AC-FS(config)# url-rule 2 url-object url-objA time-range any action deny audit
Rule 2 already exists, please delete it first
```

【Common Mistake】 -

【Platform Description】 -

6.54vid-rule

Enable virtual identity default auditing.

vid-rule audit-default-enable

Disable the default auditing function of virtual identities.

no vid-rule audit-default-enable

【Parameter Description】-

【Default Configuration】 There is no configuration by default.

【Command Mode】 Content audit policy group configuration mode

【Default Level】 14

【Usage Guide】 1: The default audit can only be configured in the default audit group named _AUDIT_DEFAULT in the policy group, and there is no such command in other policy groups.

【Configuration Example]】1: Enable virtual identity default auditing.

```
AC-FS# configure terminal
AC-FS(config)# content-policy _AUDIT_DEFAULT AC-FS(cont-
plcy-config)# vid-rule audit-default-enable AC-FS(cont-
plcy-config)# end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】-

【Common Mistake】-

【Platform Description】 -

6.55 web-bbs-rule

Enable WEB-BBS default audit function.

web-bbs-rule audit-default-enable

Disable the default audit function of WEB-BBS.

no web-bbs-rule audit-default-enable

Delete all WEB-BBS rules under the policy group.

web-bbs-rule delete-all

Exchange the priority of WEB-BBS access control rules.

web-bbs-rule priority-swap rule-id1 rule-id2

Add WEB-BBS access control rules to the content audit policy group.

web-bbs-rule rule-id time-range time-name [content content-object-name] action { permit | deny } [audit] [comment comment-string]

Delete WEB-BBS access control rules.

no web-bbs-rule rule-id

【Parameter Description】

Parameter	Description
rule-id1	The ID of Rule 1 for the priority level to be exchanged.
rule-id2	The ID of Rule 2 for the priority level to be exchanged.
rule-id	ID identification of the rule, the value range (1~200), and a rule capacity of 200.
time-name	Time object name that represents the rule effective time period.
content-object-name	The content object name used by the rule.
comment-string	Description of the rule

【Default Configuration】 There is no configuration by default.

【Command Mode】 Content audit policy group configuration mode

【Default Level】 14

【Usage Guide】 1: The rule-id of a rule is not allowed to be repeated in the same content audit policy group, but is allowed to be repeated in different content audit policy groups.

2: The access control rules in a content audit policy group have corresponding priorities, and the rule assigned last has the highest priority.

3: The time-name and content-object-name associated with the rule may not exist, and the rule will not take effect at this time.

4: The swap priority command is used to swap the priorities of two access control rules. After running this command, you can see that the order of the two rules has changed in show running-config, but the order of the two rules will not appear in show running-config. Order.

5: The default audit can only be configured in the default audit group named _AUDIT_DEFAULT in the policy group, and this command will not take effect if configured in other policy groups.

【Configuration Example]】1: Enable WEB-BBS default auditing.

```
AC-FS# configure terminal
AC-FS(config)# content-policy _AUDIT_DEFAULT
AC-FS(cont-plcy-config)# web-bbs-rule audit-default-enable
AC-FS(cont-plcy-config)# end
```

2: Delete all WEB-BBS rules in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# web-bbs-rule delete-all
AC-FS(cont-plcy-config)# end
```

3: Exchange the priority of WEB-BBS access control rule 10 and rule 20 in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# web-bbs-rule priority-swap 10 20
AC-FS(cont-plcy-config)# end
```

4: Add a WEB-BBS access audit rule to the content audit policy group policyA, filter users to browse WEB-BBS content, and need to audit the browsing information.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# web-bbs-rule priority-swap 10 20
AC-FS(cont-plcy-config)# end
```

```
comment DenyInvalidBBS
AC-FS(cont-plcy-config)# end
```

【Verification】Use the show running-config command to view the configuration status.

【Prompt Information】1: If the configured rule-id already exists, a prompt will be given.

```
AC-FS(config)# web-bbs-rule 2 time-range any content keyword-group action deny audit comment
DenyInvalidBBS
Rule 2 already exists, please delete it first
```

【Common Mistake】-

【Platform Description】 -

6.56 web-mail-rule

Enable WEB-MAIL default audit function.

web-mail-rule audit-default-enable

Disable the default audit function of WEB-MAIL.

no web-mail-rule audit-default-enable

Delete all WEB-MAIL rules under the policy group.

web-mail-rule delete-all

Exchange the priority of WEB-MAIL access control rules.

web-mail-rule priority-swap rule-id1 rule-id2

Add the public part of the WEB-MAIL access control rule to the content audit policy group.

web-mail-rule rule-id time-range time-name [direction { in | out | double }] action { permit | deny } audit [comment comment-string]

Add a further parameter description of the WEB-MAIL access control rule to the content audit policy group, mainly the keyword matching conditions of the Description rule. This command is optional, if not configured, it means audit all mail information that satisfies the web-mail-rule rule-id time-range command.

web-mail-rule rule-id relation { and | or } [from content-object-name1] [to content-object-name2] [subject content-object-name3] [body content-object-name4] [attachment-name content-object-name5]

Delete the WEB-MAIL access control rule.

no web-mail-rule rule-id

【Parameter Description】

Parameter	Description
rule-id1	The ID of Rule 1 for the priority level to be exchanged.
rule-id2	The ID of Rule 2 for the priority level to be exchanged.
rule-id	ID identification of the rule, the value range (1~200), and a rule capacity of 200.
time-name	Time object name that represents the rule effective time period.
comment-string	The rule of the Description.
content-object-name1	From the sender keyword, the missing item means that it is not required to match it.
content-object-name2	Recipient keyword, missing item does not match.
content-object-name3	Message title keyword, the missing item indicates that the item is not matched.
content-object-name4	Message content keyword, the missing item means that the item is not matched.
content-object-name5	Attachment name keyword, missing item indicates that the item does not match.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Content audit policy group configuration mode

【Default Level】 14

【Usage Guide】 1: The rule-id of a rule is not allowed to be repeated in the same content audit policy group, but is allowed to be repeated in different content audit policy groups.

2: The access control rules in a content audit policy group have corresponding priorities, and the rule assigned last has the highest priority.

3: The time-name and content-object-name associated with the rule may not exist, and the rule will not take effect at this time. 4: When the rule is configured as blocking, only the or relation in relation will be valid.

5: The swap priority command is used to swap the priorities of two access control rules. After running this command, you can see that the order of the two rules has changed in show running-config, but the order of the two rules will not appear in show running-config. Order.

6: The default audit can only be configured in the default audit group whose policy group name is _AUDIT_DEFAULT, and this command will not take effect if configured in other policy groups.

【Configuration Example]】 1: Enable WEB-MAIL default auditing.

```
AC-FS# configure terminal
AC-FS(config)# content-policy _AUDIT_DEFAULT
AC-FS(cont-plcy-config)# web-mail-rule audit-default-enable
AC-FS(cont-plcy-config)# end
```

2: Delete all WEB-MAIL rules in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# web-mail-rule delete-all
AC-FS(cont-plcy-config)# end
```

3: Exchange the priority of WEB-MAIL access control rule 10 and rule 20 in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# web-mail-rule priority-swap 10 20
AC-FS(cont-plcy-config)# end
```

4: Add a WEB-MAIL access control rule to the content audit policy group policyA, allowing users to send WEB mail, matching OBJ-F to the sender. eyword, or subject matching OBJ-S keywords.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# web-mail-rule 1 time-range any action permit audit comment mail-audit-1
AC-FS(cont-plcy-config)# web-mail-rule 1 relation or from OBJ-F subject OBJ-S
AC-FS(cont-plcy-config)# end
```

【Verification】 Use the show running-config command to view the configuration status.

【Prompt Information】 1: If the configured rule-id already exists, a prompt will be given.

```
AC-FS(config)# web-mail-rule 1 time-range any action permit audit comment mail-audit-1
Rule 1 already exists, please delete it first
```

2: If the public part of the rule is not configured, and the further Description of the rule is directly configured, a prompt will be given.

```
AC-FS(config)# web-mail-rule 1 relation or from OBJ-F subject OBJ-S
Rule 1 is not exist
```

【Common Mistake】 -

【Platform Description】 -

6.57 web-search-rule

Enable WEB-SEARCH default audit function.

web-search-rule audit-default-enable

Turn off the default audit function of WEB-SEARCH.

no web-search-rule audit-default-enable

Delete all WEB-SEARCH rules under the policy group.

web-search-rule delete-all

Exchange the priority of WEB-SEARCH access control rules.

web-search-rule priority-swap rule-id1 rule-id2

Add a WEB-SEARCH access control rule to the content audit policy group.

web-search-rule rule-id time-range time-name [content content-object-name] action { permit | deny } [audit] [comment comment-string]

Delete the WEB-SEARCH access control rule.

no web-search-rule rule-id

【Parameter Description】

Parameter	Description
rule-id1	The ID of Rule 1 for the priority level to be exchanged.
rule-id2	The ID of Rule 2 for the priority level to be exchanged.
rule-id	ID identification of the rule, value range (1~200), and rule capacity of 200.
time-name	Time object name that represents the rule effective time period.
content-object-name	The content object name used by the rule.
comment-string	The rule of the Description.

【Default Configuration】 There is no configuration by default.

【Command Mode】 Content audit policy group configuration mode

【Default Level】 14

【Usage Guide】 1: The rule-id of a rule is not allowed to be repeated in the same content audit policy group, but is allowed to be repeated in different content audit policy groups.

2: The access control rules in a content audit policy group have corresponding priorities, and the rule assigned last has the highest priority.

3: The time-name and content-object-name associated with the rule may not exist, and the rule will not take effect at this time.

4: The swap priority command is used to swap the priorities of two access control rules. After running this command, you can see that the order of the two rules has changed in show running-config, but the order of the two rules will not appear in show running-config. Order.

5: The default audit can only be configured in the default audit group named _AUDIT_DEFAULT in the policy group, and this command will not take effect if configured in other policy groups.

【Configuration Example]】 1: Enable WEB-SEARCH default auditing.

```
AC-FS# configure terminal
AC-FS(config)# content-policy _AUDIT_DEFAULT
AC-FS(cont-plcy-config)# web-search-rule audit-default-enable
AC-FS(cont-plcy-config)# end
```

2: Delete all WEB-SEARCH rules in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# web-search-rule delete-all
AC-FS(cont-plcy-config)# end
```

3: Exchange the priority of WEB-SEARCH access control rule 10 and rule 20 in policy group policyA.

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# web-search-rule priority-swap 10 20
AC-FS(cont-plcy-config)# end
```

4: Add a WEB-SEARCH access audit rule to the content audit policy group policyA to filter the behavior of users searching for keywords in the keyword-group content object, and the search information needs to be audited

```
AC-FS# configure terminal AC-FS(config)#
content-policy policyA
AC-FS(cont-plcy-config)# web-search-rule 2 time-range any content keyword-group action deny audit
comment DenyInvalidSearch
AC-FS(cont-plcy-config)# end
```

【Verification】 Use the show running-config command to view the configuration status.

【Prompt Information】 1: If the configured rule-id already exists, a prompt will be given.

```
AC-FS(config)# web-search-rule 2 time-range any content keyword-group action deny audit comment
DenyInvalidSearch
Rule 2 already exists, please delete it first
```

【Common Mistake】-

【Platform Description】-