

FiberstoreOS

Security Command Line Reference

1 Port Security Commands.....	8
1.1 clear port-security address-table static.....	8
1.2 switchport port-security.....	8
1.3 switchport port-security mac-address.....	9
1.4 switchport port-security maximum.....	10
1.5 switchport port-security violation.....	10
1.6 show port-security address-table.....	11
1.7 show port-security current mac-num interface.....	12
1.8 show port-security interface.....	12
1.9 show port-security maximum mac-num interface.....	13
2 Vlan Security Commands.....	14
2.1 vlan mac-limit maximum.....	14
2.2 vlan mac-limit action.....	14
2.3 vlan mac learning.....	15
2.4 show vlan-security.....	16
3 Time Range Commands.....	17
3.1 time-range.....	17
3.2 absolute.....	17
3.3 periodic.....	18
3.4 show time-range.....	19
4 ACL Commands.....	20
4.1 mac access-list.....	20
4.2 sequence-num.....	20
4.3 deny src-mac.....	21
4.4 permit src-mac.....	23
4.5 remark.....	24
4.6 show access-list mac.....	24
4.7 ip access-list.....	25
4.8 deny.....	26
4.9 deny tcp.....	27
4.10 deny udp.....	29
4.11 deny icmp.....	29
4.12 deny igmp.....	30

4.13 permit.....	31
4.14 permit tcp.....	32
4.15 permit udp.....	33
4.16 permit icmp.....	33
4.17 permit igmp.....	34
4.18 show access-list ip.....	34
5 Extend ACL Commands.....	36
5.1 ip access-list extend.....	36
5.2 sequence-num.....	37
5.3 deny src-mac.....	37
5.4 permit src-mac.....	39
5.5 deny.....	40
5.6 deny tcp.....	41
5.7 deny udp.....	43
5.8 deny icmp.....	43
5.9 deny igmp.....	44
5.10 permit.....	45
5.11 permit tcp.....	45
5.12 permit udp.....	46
5.13 permit icmp.....	47
5.14 permit igmp.....	47
5.15 remark.....	48
5.16 show access-list ip.....	49
6 ACLv6 Commands.....	50
6.1 ipv6 access-list.....	50
6.2 sequence-num.....	50
6.3 remark.....	51
6.4 show access-list ipv6.....	52
6.5 deny.....	52
6.6 deny tcp.....	53
6.7 deny udp.....	54
6.8 deny icmp.....	55
6.9 permit.....	56
6.10 permit tcp.....	57
6.11 permit udp.....	58
6.12 permit icmp.....	58
7 IEEE 802.1x Commands.....	60

7.1 dot1x system-auth-ctrl.....	60
7.2 dot1x initialize.....	60
7.3 dot1x max-reauth-req.....	61
7.4 dot1x port-control.....	62
7.5 dot1x protocol-version.....	63
7.6 dot1x quiet-period.....	63
7.7 dot1x reauthentication.....	64
7.8 dot1x re-authenticate.....	64
7.9 dot1x timeout.....	65
7.10 dot1x guest-vlan.....	66
7.11 radius-server deadtime.....	67
7.12 radius-server host.....	68
7.13 radius-server retransmit.....	69
7.14 radius-server timeout.....	69
7.15 radius-server key.....	70
7.16 show dot1x.....	71
7.17 debug dot1x.....	71
7.18 clear dot1x.....	72
7.19 show radius-server.....	73
7.20 dot1x re-active radius-server.....	74
8 Arp Inspection Commands.....	75
8.1 show ip arp inspection.....	75
8.2 show ip arp inspection interfaces.....	76
8.3 show ip arp inspection log.....	77
8.4 show ip arp inspection statistics.....	78
8.5 show ip arp inspection vlan.....	79
8.6 show debugging arp inspection.....	79
8.7 debug arp inspection.....	80
8.8 ip arp inspection filter vlan.....	80
8.9 ip arp inspection log-buffer entries.....	81
8.10 [no] ip arp inspection log-buffer logs interval.....	82
8.11 ip arp inspection validate.....	82
8.12 ip arp inspection vlan.....	83
8.13 ip arp inspection vlan logging acl-macth.....	83
8.14 ip arp inspection vlan logging dhcp-bindings.....	84
8.15 clear ip arp inspection log-buffer.....	85
8.16 clear ip arp inspection statistics.....	85
8.17 ip arp inspection trust.....	86

8.18 arp access-list.....	86
8.19 ip mac.....	87
8.20 no sequence-num.....	87
8.21 show access-list arp.....	88
9 DHCP Snooping Commands.....	90
9.1 clear dhcp snooping.....	90
9.2 dhcp snooping.....	90
9.3 dhcp snooping binding.....	91
9.4 dhcp snooping database.....	92
9.5 dhcp snooping information option.....	93
9.6 dhcp snooping information option allow-untrusted.....	94
9.7 dhcp snooping trust.....	94
9.8 dhcp snooping verify.....	95
9.9 dhcp snooping vlan.....	96
9.10 dhcp snooping vlan information option format-type circuit-id string.....	96
9.11 dhcp snooping information option format remote-id.....	97
9.12 debug dhcp snooping.....	98
9.13 show dhcp snooping binding.....	98
9.14 show dhcp snooping config.....	99
9.15 show dhcp snooping statistics.....	100
9.16 show dhcp snooping trusted-sources.....	100
10 IP Source Guard Commands.....	102
10.1 ip source binding.....	102
10.2 no ip source binding.....	103
10.3 ip source maximal binding.....	103
10.4 ip verify source.....	104
10.5 show ip source binding.....	105
11 RADIUS Authentication Commands.....	106
11.1 aaa new-model.....	106
11.2 aaa authentication login.....	106
11.3 aaa authorization exec.....	107
11.4 aaa accounting exec.....	108
11.5 aaa accounting commands.....	109
11.6 aaa privilege mapping.....	109
11.7 login authentication.....	110
11.8 authorization exec.....	111
11.9 accounting exec.....	111

11.10 accounting commands.....	112
11.11 show aaa method-lists authentication.....	112
11.12 show aaa status.....	113
11.13 show aaa privilege mapping.....	114
12 Tacacs+ Commands.....	115
12.1 tacacs-server host.....	115
12.2 clear tacacs statistics.....	115
12.3 show tacacs.....	116
13 Port Isolate Commands.....	118
13.1 port-isolate group.....	118
13.2 port-isolate mode.....	118
13.3 show port-isolate.....	119
14 Private Vlan Commands.....	121
14.1 switchport mode private-vlan.....	121
14.2 switchport private-vlan.....	121
14.3 show private-vlan.....	122
15 DDOS Commands.....	124
15.1 ip icmp intercept.....	124
15.2 ip smurf intercept.....	124
15.3 ip fraggle intercept.....	125
15.4 ip udp intercept.....	125
15.5 ip tcp intercept.....	126
15.6 ip small-packet intercept.....	127
15.7 ip maceq intercept.....	127
15.8 ip ipeq intercept.....	128
15.9 show ip-intercept config.....	128
15.10 show ip-intercept config.....	129
15.11 show ip-intercept statistics.....	130
15.12 clear ip-intercept statistics.....	130
16 Key Chain Commands.....	132
16.1 key chain.....	132
16.2 key.....	132
16.3 key-string.....	133
16.4 accept-lifetime.....	134
16.5 send-lifetime.....	134
16.6 show key chain.....	135

17 Port-block Commands.....	137
17.1 port-block.....	137
17.2 show port-block.....	138

1 Port Security Commands

1.1 clear port-security address-table static

Use this command to clear static port-security mac address table.

Command Syntax

clear port-security address-table static (**address** *address* | **interface** *interface* | **vlan** *vlan* /)

address <i>address</i>	Clear port-security entries with specified mac address
interface <i>interface</i>	Clear port-security entries with specified interface name
vlan <i>vlan</i>	Clear port-security entries with specified vlan id

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to clear static port-security mac address-table.

```
Switch# clear port-security address-table static
```

This example shows how to clear static port-security mac address-table on eth-0-1.

```
Switch# clear port-security address-table static interface eth-0-1
```

Related Commands

show mac address-table

1.2 switchport port-security

To enable port security on an interface, use the switchport port-security command. To disable port security, use the no form of this command.

Command Syntax

switchport port-security

no switchport port-security

Command Mode

Interface Configuration

Default

Disabled

Usage

When disable port-security, all the port-security mac address entries which are learnt dynamically will be cleared. The static port-security mac address will be ineffective but not be cleared

Examples

This example shows how to enable port security on an interface.

```
Switch(config-if)# switchport port-security
```

This example shows how to disable port security on an interface.

```
Switch(config-if)# no switchport port-security
```

Related Commands

show port-security interface

1.3 switchport port-security mac-address

Use this command to add static port-security mac address.

Command Syntax

switchport port-security mac-address *address* *vlan* *vlan*

no switchport port-security mac-address *address* *vlan* *vlan*

<i>address</i>	Static port-security mac address
<i>vlan</i>	Static port-security vlan id

Command Mode

Interface Configuration

Default

None

Usage

None

Examples

This example shows how to configure static port-security mac address.

```
Switch(config-if)# switchport port-security mac-address 0.0.1 vlan 1
```

This example shows how to delete static port-security mac address.

```
Switch(config-if)# no switchport port-security mac-address 0.0.1 vlan 1
```

Related Commands

show mac address-table

1.4 switchport port-security maximum

Use this command to set the maximum of secure MAC addresses on a port. Use the no form of this command to return to the default settings.

Command Syntax

switchport port-security maximum *maximum*

no switchport port-security maximum

<i>maximum</i>	Maximum number of secure MAC addresses for the interface; valid values are from 1 to 16384
----------------	--

Command Mode

Interface Configuration

Default

1

Usage

If the new input maximum is smaller than the current secure addresses on the interface, the command is rejected.

Once the maximum number of secure MAC addresses on the port is reached, no more addresses are learnt on that port

Examples

This example sets the maximum number of secure MAC addresses on a port.

```
Switch(config-if)# switchport port-security maximum 1024
```

This example restores the maximum number of secure MAC addresses on a port to default value.

```
Switch(config-if)# no switchport port-security maximum
```

Related Commands

switchport port-security violation

show port-security maximum mac-num interface *IFNAME*

1.5 switchport port-security violation

Use this command to set the action to be taken when a security violation is detected. Use the no form of this command to return to the default settings.

Command Syntax

switchport port-security violation (protect | restrict | errdisable)

no switchport port-security violation

protect	Discard packet silently
restrict	Discard packet and print log
errdisable	Discard packet, log and set the interface error-disabled

Command Mode

Interface Configuration

Default

Discard packet silently

Usage

To use this command, enable switchport port-security first

Examples

This example sets port-security violation to discard packets silently.

```
Switch(config-if) # switch port-security violation protect
```

Related Commands

switchport port-security

1.6 show port-security address-table

Use this command to show port-security mac address-table.

Command Syntax

show port-security address-table (dynamic | static |) (address *address* | interface *interface* | vlan *vlan* |)

dynamic	Show the dynamically learnt entries
static	Show the statically configured entries
address <i>address</i>	Show the entries with specified mac address
interface <i>interface</i>	Show the entries with specified interface name
vlan <i>vlan</i>	Show the entries with specified vlan id

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows port-security mac address-table on the Switch.

```
Switch# show port-security address-table
Secure Mac Address Table
-----
Vlan    Mac Address                Type                Ports
-----
1       0001.00ce.ef01            SecureConfigured    eth-0-11
41      001a.a02c.a1dc            SecureConfigured    eth-0-41
```

Related Commands

None

1.7 show port-security current mac-num interface

Use this command to show current port-security mac-num on interface.

Command Syntax

show port-security current mac-num interface *interface*

<i>interface</i>	Show the entries with specified interface name
------------------	--

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows current port-security mac-num on interface eth-0-1.

```
Switch# show port-security current mac-num interface eth-0-1
Current MAC Addresses : 1
```

Related Commands

switchport port-security maximum

show port-security maximum mac-num interface *interface*

1.8 show port-security interface

Use this command to show the port-security information on an interface.

Command Syntax

show port-security interface *interface*

<i>interface</i>	Show the entries with specified interface name
------------------	--

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows the port-security information on interface eth-0-1.

```
Switch# show port-security interface eth-0-1
Port Security          : disabled
Violation mode        : discard packet silence
Maximum MAC Addresses  : 1
Total MAC Addresses   : 1
Static configured MAC Addresses : 1
```

Related Commands

None

1.9 show port-security maximum mac-num interface

Use this command to show the port-security maximum mac-num on an interface.

Command Syntax

show port-security maximum mac-num interface *interface*

<i>interface</i>	Show the entries with specified interface name
------------------	--

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows the port-security maximum mac-num on interface eth-0-1.

```
Switch# show port-security maximum mac-num interface eth-0-1
Maximum MAC Addresses : 1024
```

Related Commands

switchport port-security maximum

show port-security current mac-num interface

2 Vlan Security Commands

2.1 vlan mac-limit maximum

Use this command to set/unset maximum of mac addresses in specified vlan.

Command Syntax

vlan *VLAN-ID* **mac-limit maximum** *maximum*

no vlan *VLAN-ID* **mac-limit maximum**

<i>vlan-id</i>	vlan id, between 1 and 4094
<i>maximum</i>	maximum of mac addresses, between 1 and 65535

Command Mode

Vlan Configuration

Defaults

No mac-limit on all vlans

Usage

The vlan must be created before this command

Examples

This example shows how to set/unset maximum of mac addresses for specified vlan

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config-vlan)# vlan 2 mac-limit maximum 1000
Switch(config-vlan)# no vlan 2 mac-limit maximum
```

Related Commands

show vlan-security

2.2 vlan mac-limit action

Use this command to set/unset action for specified vlan.

Command Syntax

vlan *VLAN-ID* **mac-limit action** (**discard**|**warn**|**forward**)

no vlan *VLAN-ID* **mac-limit action**

<i>vlan-id</i>	vlan id, between 1 and 4094
discard	If the count of mac addresses reaches the maximum, packets with unknown source mac address from this vlan will be discarded
warn	If the count of mac addresses reaches the maximum, packets with unknown source mac address from this vlan will be discarded, and warning log will be printed in syslog
forward	If the count of mac addresses reaches the maximum, all packets from this vlan will be forwarded without mac learning nor warning log

Command Mode

Vlan Configuration

Defaults

Forward

Usage

The vlan must be created before this command.

Examples

This example shows how to set/unset action for specified vlan :

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config-vlan)# vlan 2 mac-limit action warn
Switch(config-vlan)# no vlan 2 mac-limit action
```

Related Commands

show vlan-security

2.3 vlan mac learning

Use this command to enable/disable mac learning for specified vlan.

Command Syntax

vlan *VLAN-ID* mac learning (enable|disable)

<i>vlan-id</i>	vlan id, between 1 and 4094
enable	Enable learning
disable	Disable learning

Command Mode

Vlan Configuration

Defaults

Enable

Usage

The vlan must be created before this command.

Examples

This example shows how to enable mac learning for specified vlan

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config-vlan)# vlan 2 mac learning enable
```

Related Commands

show vlan-security

2.4 show vlan-security

Use this command to show configuration about vlan security.

Command Syntax

show vlan-security (vlan *VLAN-ID*)

vlan <i>vlan-id</i>	vlan id, between 1 and 4094
----------------------------	-----------------------------

Command Mode

EXEC mode

Defaults

None

Usage

None

Examples

This example shows how to show configuration about vlan security

```
Switch# configure terminal
Switch(config)# vlan database
Switch(config-vlan)# vlan 2
Switch(config-vlan)# vlan 2 mac-limit maximum 1000
Switch(config-vlan)# vlan 2 mac-limit action warn
Switch # show vlan-security
Vlan learning-en max-mac-count cur-mac-count action
-----
2 Enable 1000 0 Warn
```

Related Commands

vlan mac-limit maximum

vlan mac-limit action

vlan mac learning

3 Time Range Commands

3.1 time-range

Use this command to create time range and enter time-range configuration mode.

Command Syntax

time-rang *TIME-RANGE-NAME*

no time-rang

<i>TIME-RANGE-NAME</i>	the name of the time range, up to 20 characters
------------------------	---

Command Mode

Global Configuration

Default

None

Usage

A time range is used to determine a range of time during which a filter is effective.

Examples

This example shows how to create a time range with the name “my-time-range”.

```
Switch(config)# time-range my-time-range
Switch(config-tm-range)#
```

Related Commands

show time-range

3.2 absolute

Use this command to define the absolute time and date in time range.

Command Syntax

absolute (**start** *HH:MM:SS MONTH <1-31> <2000-2037>*) (**end** *HH:MM:SS MONTH <1-31> <2000-2037>*)

start	Starting time and date
end	Ending time and date
HH:MM:SS	Starting time or Ending time

MONTH <1-31>	Day of the month
<2000-2037>	Year

Command Mode

Time range Configuration

Default

None

Usage

Comparing with the periodic time, choose an appropriate type.

Examples

This example shows how to define a time range started from 11:11:00 January 1 2008 and ended by 00:00:00 May 1 2009.

```
Switch(config-tm-range)# absolute start 11:11:00 jun 1 2008 end 00:00:00 may 1 2009
```

Related Commands

periodic

3.3 periodic

Use this command to define the periodic time and date in time range.

Command Syntax

periodic *HH:MM WEEKDAY to HH:MM (WEEKDAY)*

periodic *HH:MM (weekdays | weekend | daily) to HH:MM*

HH:MM	Starting time or Ending time
weekdays	Monday thru Friday
weekend	Saturday and Sunday
daily	Every day of the week
WEEKDAY	Day of the week(First three letters of the weekday)

Command Mode

Time range Configuration

Default

None

Usage

Comparing with the absolute time, choose an appropriate type.

Examples

This example shows how to define a time range started from 00:00 Monday and ended by 18:00 Wednesday in weekly period.

```
Switch(config-tm-range)# periodic 00:00 mon to 18:00 wed
```

This example shows how to define a time range started from 09:00 and ended by 17:00 every day.

```
Switch(config-tm-range)# periodic 09:00 daily to 17:00
```

Related Commands

absolute

3.4 show time-range

Use this command to show the information of time-range.

Command Syntax

show time-range (*TIME-RANGE-NAME*)

<i>TIME-RANGE-NAME</i>	the name of the time range, up to 20 characters. Show all the time ranges when the name is not specified
------------------------	--

Command Mode

Privileged EXEC

Default

None

Usage

If no time range is specified, all time-ranges in the system should be shown.

Examples

This example shows how to display the information of all the time ranges.

```
Switch# show time-range
time-range rangel
    periodic 00:01 weekdays to 12:01
```

Related Commands

time-range

4 ACL Commands

4.1 mac access-list

Use this command to create MAC ACL and then enter MAC ACL in global configuration mode.

Command Syntax

mac access-list *ACL-NAME*

no mac access-list *ACL-NAME*

<i>ACL-NAME</i>	The name of the MAC ACL
-----------------	-------------------------

Command Mode

Global Configuration

Default

None

Usage

If the system already has a MAC ACL with the same name, this command will enter the MAC ACL configuration mode. However, if the ACL name is used by other type of ACL, a prompt message will be shown.

When the name is not used by any ACL, this command is to create the MAC ACL firstly and then enter the MAC ACL configuration mode.

Examples

This example shows how to create a MAC ACL named list_mac_1 and then enter the MAC ACL configuration mode.

```
Switch(config)# mac access-list list_mac_1
Switch(config-mac-acl)#
```

This example shows how to remove the MAC ACL named list_mac_1.

```
Switch(config)# no mac access-list list_mac_1
```

Related Commands

match access-group

4.2 sequence-num

Use this command to remove a filter from MAC ACL.

Command Syntax

no sequence-num *SEQUENCE-NUM*

<i>SEQUENCE-NUM</i>	The sequence number of a MAC filter, the range is 1 to 131071
---------------------	---

Command Mode

MAC ACL Configuration or IP ACL configuration

Default

None

Usage

None

Examples

This example shows how to remove a filter with the sequence-num 10 from MAC ACL.

```
Switch(config-mac-acl)# no sequence-num 10
```

Related Commands

deny

deny tcp

deny udp

deny icmp

deny igmp

permit

permit tcp

permit udp

permit icmp

permit igmp

4.3 deny src-mac

Use this command to create a MAC filter for discarding ongoing packets matching the filter rule.

Command Syntax

(SEQUENCE-NUM |) **deny src-mac** (**any** | *MAC MASK* | **host** *MAC*) (**dest-mac** (**any** | *MAC MASK* | **host** *MAC*) |) (**untag-vlan** | ((**vlan** *VLAN* |) (**cos** *VALUE* |) (**inner-vlan** *VLAN* |) (**inner-cos** *VALUE* |)) (**protocol** (**arp** (**arp-op-code**) | **rarp**) |) (**time-range** *TIME-RANGE-NAME* |)

<i>SEQUENCE-NUM</i>	The sequence number of the filter in MAC ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented. The range is 1 to 131071
---------------------	---

any	Any host
<i>MAC MASK</i>	The MAC address and its wildcard bits
host MAC	The host with a specified MAC address
dest-mac	Destination MAC address
untag-vlan	Without vlan tag
vlan VLAN	VLAN-ID, the range is 1 to 4094
cos VALUE	CoS, the range is 0 to 7
inner-vlan VLAN	Inner VLAN-ID, the range is 1 to 4094
inner-cos VALUE	Inner CoS, the range is 0 to 7
protocol	The protocol type which including ARP, RARP or Ether type
arp	ARP 协议
arp-op-code	arp-op-code,范围是 0~65535
rarp	RARP 协议
time-range <i>TIME-RANGE-NAME</i>	The time-range used by the MAC filter

Command Mode

MAC ACL Configuration

Default

None

Usage

An auto-generated sequence number will be assigned to the filter if the sequence-num field is not presented. The auto-generated sequence number is incremented by 10 on the maximum existing sequence number in the MAC ACL. i.e. when the maximum existing sequence number is 100, the sequence number of subsequent created MAC filter is 110. Eth-type is not supported in egress ACL.

Examples

This example shows how to create a filter in MAC ACL to deny the packets with source MAC address 001A.A02C.A1DF.

```
Switch(config-mac-acl)# 1 deny src-mac host 001A.A02C.A1DF
```

This example shows how to create a filter in MAC ACL to deny all the packets.

```
Switch(config-mac-acl)# 2 deny src-mac any
```

This example shows how to create a filter in MAC ACL to deny the packet whose source MAC address is between the ranges specified.

```
Switch(config-mac-acl)# 3 deny src-mac 001A.A02C.A1DF 001A.A02C.0000
```

Related Commands

no sequence-num

4.4 permit src-mac

Use this command to create a MAC filter for allowing packets matching the filter rule to be delivered.

Command Syntax

```
(SEQUENCE-NUM | ) permit src-mac (any | MAC MASK | host MAC) ( dest-mac (any | MAC MASK | host MAC) | ) ( untag-vlan | ( vlan VLAN | ) ) ( cos VLAN | ) ( inner-vlan VLAN | ) ( inner-cos VALUE | ) ) ( protocol (arp ( arp-op-code ) | rarp ) | ) ( time-range TIME-RANGE-NAME | )
```

<i>SEQUENCE-NUM</i>	The sequence number of the filter in MAC ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented. The range is 1 to 2147483646
any	Any host
<i>MAC MASK</i>	The MAC address and its wildcard bits
host <i>MAC</i>	The host with a specified MAC address
dest-mac	Destination MAC address
untag-vlan	Without vlan tag
vlan <i>VLAN</i>	VLAN-ID, the range is 1 to 4094
cos <i>VALUE</i>	CoS, the range is 0 to 7
inner-vlan <i>VLAN</i>	Inner VLAN-ID, the range is 1 to 4094
inner-cos <i>VALUE</i>	Inner CoS, the range is 0 to 7
protocol	The protocol type which including ARP, RARP
arp	ARP 协议
arp-op-code	arp-op-code,范围是 0~65535
rarp	RARP 协议
time-range <i>TIME-RANGE-NAME</i>	The time-range used by the MAC filter

Command Mode

MAC ACL Configuration

Default

None

Usage

An auto-generated sequence number will be assigned to the filter if the sequence-num field is not presented. The auto-generated sequence number is incremented by 10 on the maximum existing sequence number in the MAC ACL. i.e. when the maximum existing sequence number is 105, the sequence number of subsequent created MAC filter is 115. Eth-type is not supported in egress ACL.

Examples

This example shows how to create a filter in MAC ACL to permit the packets with source MAC address 001A.A02C.A1DF.

```
Switch(config-mac-acl)# 1 permit src-mac host 001A.A02C.A1DF
```

This example shows how to create a filter in MAC ACL to permit all the packets.

```
Switch(config-mac-acl)# 2 permit src-mac any
```

This example shows how to create a filter in MAC ACL to permit the packets with source MAC address between the ranges specified.

```
Switch(config-mac-acl)# 3 permit src-mac 001A.A02C.A1DF 001A.A02C.0000
```

Related Commands

no sequence-num

4.5 remark

Use this command to add remarks for the MAC ACL.

To remove remarks of the MAC ACL, use the no form of this command.

Command Syntax

remark *REMARK*

no remark

<i>REMARK</i>	The remarks of the MAC ACL
---------------	----------------------------

Command Mode

MAC ACL Configuration or IP ACL configuration

Default

None

Usage

The remarks are up to 100 characters. The exceed parts will not be stored and will be truncated.

Examples

This example shows how to add a remark to describe the MAC ACL.

```
Switch(config-mac-acl)# remark remark of List for mac
```

This example shows how to remove the remark of the MAC ACL.

```
Switch(config-mac-acl)# no remark
```

Related Commands

mac access-list

4.6 show access-list mac

Use this command to show the MAC ACL information.

Command Syntax

show access-list mac (*ACL-NAME* |)

<i>ACL-NAME</i>	The name of the MAC ACL
-----------------	-------------------------

Command Mode

Privileged EXEC

Default

None

Usage

If no mac acl are specified, all mac access-lists in the system should be shown.

Examples

This example shows how to show the MAC ACL information.

Switch# show access-list mac

```
mac access-list list_mac_1
 10 deny src-mac host 0000.0001.0002
 20 permit src-mac any
```

Related Commands

mac access-list

4.7 ip access-list

Use this command to create IP ACL and then enter IP ACL configuration mode.

To remove this ACL, use the no form of this command.

Command Syntax

ip access-list *ACL-NAME*

no ip access-list *ACL-NAME*

<i>ACL-NAME</i>	The name of an IP ACL
-----------------	-----------------------

Command Mode

Global Configuration

Default

None

Usage

If the system already has an IP ACL with the same name, this command will enter the IP ACL configuration mode. However, if the ACL name is used by other type of ACL, a prompt message will be shown.

When the name is not used by any ACL, this command is to create the IP ACL firstly and then enter the IP ACL configuration mode.

Examples

This example shows how to create an IP ACL named list_ipv4_1 and then enter the IP ACL configuration mode.

```
Switch(config)# ip access-list list_ipv4_1
Switch(config-ip-acl)#
```

This example shows how to remove the IP ACL named list_ipv4_1.

```
Switch(config)# no ip access-list list_ipv4_1
```

Related Commands

match access-group

4.8 deny

Use this command to discard ongoing IP packets matching the IP filter.

Command Syntax

(SEQUENCE-NUM |) **deny** (*PROTO-NUM | any*) (*SOURCE SOURCE-MASK | any | host SOURCE*) (*DESTINATION DESTINATION-MASK | any | host DESTINATION*) (**ip-precedence** *PRECEDENCE | dscp DSCP |*) (**non-fragment|first-fragment|non-or-first-fragment|small-fragment|non-first-fragment**) (**routed-packet** |) (*options* |) (**time-range** *TIME-RANGE-NAME* |)

<i>SEQUENCE-NUM</i>	The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented. The range is 1 to 131071
<i>PROTO-NUM</i>	An IP protocol number, the range is 0 to 255
any	Any IP protocol
<i>SOURCE SOURCE-MASK</i>	The source IP address and its wildcard bits
any	Any source host
host <i>SOURCE</i>	The source IP address of a host
<i>DESTINATION DESTINATION-MASK</i>	The destination IP address and its wildcard bits
any	Any destination host
host <i>DESTINATION</i>	The destination IP address of a host
ip-precedence <i>PRECEDENCE</i>	Match packets with given precedence value, the range is 0 to 7
dscp <i>DSCP</i>	Match packets with given dscp value, the range is 0 to 63
non-fragment	Match packets with non fragment
first-fragment	Match packets with first fragment
non-or-first-fragment	Match packets with non first fragment
small-fragment	Match packets with small fragment

non-first-fragment	Match packets with non first fragment
routed-packet	Match routed packet
options	Match packets with IP options
time-range <i>TIME-RANGE-NAME</i>	The time-range used by the IP filter

Command Mode

IP ACL configuration

Default

None

Usage

If IP address wildcard bit is provided, the IP address is logical-and in bitwise with the reverse bits of the wildcard bits. For example, 10.10.10.0 0.0.0.255 means the addresses from 10.10.10.0 to 10.10.10.255 are matched.

An auto-generated sequence number will be assigned to the filter if the sequence-number field is not presented. The auto-generated sequence number is incremented by 10 on the maximum existing sequence number in the IP ACL. i.e. when the maximum existing sequence number is 100, the sequence number of subsequent created IP filter is 110.

Examples

This example shows how to create a filter in IP ACL to deny any IP packets.

```
Switch(config-ip-acl)# 1 deny any any any
```

This example shows how to create a filter in IP ACL to deny the fragment packets with the source IP address 1.1.1.1.

```
Switch(config-ip-acl)# 2 deny any host 1.1.1.1 any fragments
```

This example shows how to create a filter in IP ACL to deny any routed packets.

```
Switch(config-ip-acl)# 3 deny any any any routed-packet
```

Related Commands

no sequence-num

4.9 deny tcp

Use this command to reject TCP packets matching the IP filter.

Command Syntax

```
(SEQUENCE-NUM | ) deny tcp ( SOURCE SOURCE-MASK | any | host SOURCE ) ( src-port
OPERATOR PORT | )( DESTINATION DESTINATION-MASK | any | host DESTINATION )
( dst-port OPERATOR PORT | ) ( ip-precedence PRECEDENCE | dscp DSCP | )
( established | ( match-any | match-all FLAG-NAME | ) | )
(non-fragment|first-fragment|non-or-first-fragment|small-fragment|non-first-frag
ment) ( routed-packet | ) ( options | ) ( time-range TIME-RANGE-NAME | )
```

<i>SEQUENCE-NUM</i>	The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the
---------------------	--

	filter if this field is not presented. the range is 1 to 2147483646
<i>SOURCE SOURCE-MASK</i>	The source IP address and its wildcard bits
any	Any source host
host <i>SOURCE</i>	The source IP address of a host
src-port <i>OPERATOR PORT</i>	Source port, the range is 0 to 65535. Including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range
<i>DESTINATION DESTINATION-MASK</i>	The destination IP address and its wildcard bits
any	Any destination host
host <i>DESTINATION</i>	The destination IP address of a host
dst-port <i>OPERATOR PORT</i>	Destination port, the range is 0 to 65535. Including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range
ip-precedence <i>PRECEDENCE</i>	Match packets with given precedence value, the range is 0 to 7
dscp <i>DSCP</i>	Match packets with given dscp value, the range is 0 to 63
established	Match established connections
match-any	Match any of the flag-name
match-all <i>FLAG-NAME</i>	Match all the flag-name, including ack, fin, psh, rst, syn and urg
non-fragment	Match packets with non fragment
first-fragment	Match packets with first fragment
non-or-first-fragment	Match packets with non first fragment
small-fragment	Match packets with small fragment
non-first-fragment	Match packets with non first fragment
routed-packet	Match routed packet
options	Match packets with IP options
time-range <i>TIME-RANGE-NAME</i>	The time-range used by the IP filter

Command Mode

IP ACL configuration

Default

None

Usage

The fragments will be invalid when the layer 4 information is specified (i.e. src-port).

Examples

This example shows how to create a filter in IP ACL to deny any TCP packets.

```
Switch(config-ip-acl)# 1 deny tcp any any
```

This example shows how to create a filter in IP ACL to deny the TCP packets with the source IP address 1.1.1.1, source port 0-100.

```
Switch(config-ip-acl)# 2 deny tcp host 1.1.1.1 src-port range 0 100 any
```

This example shows how to create a filter in IP ACL to deny any TCP packets in established TCP streams.

```
Switch(config-ip-acl)# 3 deny tcp any any established
```

This example shows how to create a filter in IP ACL to deny the TCP ACK packets with the source IP address 1.1.1.1.

```
Switch(config-ip-acl)# 4 deny tcp 10.10.10.0 0.0.0.0 any match-any ack
```

Related Commands

no sequence-num

4.10 deny udp

Use this command to reject UDP packets matching the IP filter.

Command Syntax

```
( SEQUENCE-NUM | ) deny udp ( SOURCE SOURCE-MASK | any | host SOURCE )  
( src-port OPERATOR PORT | )( DESTINATION DESTINATION-MASK | any | host  
DESTINATION ) ( dst-port OPERATOR PORT | ) ( ip-precedence PRECEDENCE | dscp  
DSCP | )  
( non-fragment|first-fragment|non-or-first-fragment|small-fragment|non-first-frag-  
ment ) ( routed-packet | ) ( options | ) ( time-range TIME-RANGE-NAME | )
```

Please reference to command “deny tcp” for the parameters.

Command Mode

IP ACL configuration

Default

None

Usage

The fragments will be invalid when the layer 4 information is specified (i.e. src-port).

Examples

This example shows how to create a filter in IP ACL to deny any UDP packets.

```
Switch(config-ip-acl)# 1 deny udp any any
```

This example shows how to create a filter in IP ACL to deny the UDP packets with the source IP 1.1.1.1, source port 10, and destination port less than 2000.

```
Switch(config-ip-acl)# 2 deny udp host 1.1.1.1 src-port eq 10 any dst-port lt 2000
```

Related Commands

no sequence-num

4.11 deny icmp

Use this command to reject ICMP packets matching the IP filter.

Command Syntax

```
(SEQUENCE-NUM | ) deny icmp ( SOURCE SOURCE-MASK | any | host SOURCE )
( DESTINATION DESTINATION-MASK | any | host DESTINATION ) ( icmp-type
TYPE-NUM ( icmp-code CODE-NUM | ) ) ( ip-precedence PRECEDENCE | dscp DSCP | )
(non-fragment|first-fragment|non-or-first-fragment|small-fragment|non-first-frag
ment) ( routed-packet | ) ( options | ) ( time-range TIME-RANGE-NAME | )
```

Icmp-type TYPE-NUM	ICMP message type, the range is 0 to 255
Icmp-code CODE-NUM	ICMP message code, the range is 0 to 255

Please reference to command “deny” for the parameters.

Command Mode

IP ACL configuration

Default

None

Usage

This type of filter is mostly used to reject IGMP packets.

Examples

This example shows how to create a filter in IP ACL to deny any ICMP packets.

```
Switch(config-ip-acl)# 1 deny icmp any any
```

This example shows how to create a filter in IP ACL to deny the ICMP packets with the icmp-type 3 and icmp-code 3.

```
Switch(config-ip-acl)# 2 deny icmp any any icmp-type 3 icmp-code 3
```

Related Commands

no sequence-num

4.12 deny igmp

Use this command to reject IGMP packets matching the IP filter.

Command Syntax

```
(SEQUENCE-NUM | ) deny igmp ( SOURCE SOURCE-MASK | any | host SOURCE )
( DESTINATION DESTINATION-MASK | any | host DESTINATION ) ( IGMP-TYPE | )
( ip-precedence PRECEDENCE | dscp DSCP | )
(non-fragment|first-fragment|non-or-first-fragment|small-fragment|non-first-frag
ment) ( routed-packet | ) ( options | ) ( time-range TIME-RANGE-NAME | )
```

IGMP-TYPE	IGMP type, including dvmrp, host-query, host-report, mtrace, mtrace-response, pim, precedence, trace, v2-leave, v2-report, v3-report
-----------	--

Please reference to command “deny” for the other parameters.

Command Mode

IP ACL configuration

Default

None

Usage

This type of filter is mostly used to reject IGMP packets.

Examples

This example shows how to create a filter in IP ACL to deny any IGMP packets.

```
Switch(config-ip-acl)# 1 deny igmp any any
```

This example shows how to create a filter in IP ACL to deny the IGMP packets with the source IP address 1.1.1.1, any destination IP address and the igmp-type pim.

```
Switch(config-ip-acl)# 2 deny igmp host 1.1.1.1 any pim
```

Related Commands

no sequence-num

4.13 permit

Use this command to permit packets matching the IP filter.

Command Syntax

```
(SEQUENCE-NUM | ) permit (PROTO-NUM | any) ( source SOURCE-MASK | any | host SOURCE ) (destination DESTINATION-MASK | any | host DESTINATION)  
( ip-precedence PRECEDENCE | dscp DSCP | )  
(non-fragment|first-fragment|non-or-first-fragment|small-fragment|non-first-fragment) ( routed-packet | ) ( options | ) ( time-range TIME-RANGE-NAME | )
```

Please reference to command “deny” for the parameters.

Command Mode

IP ACL configuration

Default

None

Usage

If IP address wildcard bits is provided, the IP address is logical-and in bitwise with the reverse bits of the wildcard bits. For example, 10.10.10.0 0.0.0.255 means the addresses from 10.10.10.0 to 10.10.10.255 are matched.

An auto-generated sequence number will be assigned to the filter if the sequence-num field is not presented. The auto-generated sequence number is incremented by 10 on the maximum existing sequence number in the IP ACL. i.e. when the maximum existing sequence number is 105, the sequence number of subsequent created IP filter is 115.

Examples

This example shows how to create a filter in IP ACL to permit any IP packets.

```
Switch(config-ip-acl)# 10 permit any any any
```

This example shows how to create a filter in IP ACL to permit the fragment packets with the source IP address 1.1.1.1 and any destination IP address.

```
Switch(config-ip-acl)# 20 permit tcp host 1.1.1.1 any fragments
```

This example shows how to create a filter in IP ACL to permit any routed packets.

```
Switch(config-ip-acl)# 30 permit any any any routed-packet
```

Related Commands

no sequence-num

4.14 permit tcp

Use this command to permit TCP packets matching the IP filter.

Command Syntax

```
(SEQUENCE-NUM | ) permit tcp (source SOURCE-MASK | any | host SOURCE ) ( src-port OPERATOR PORT | ) ( DESTINATION DESTINATION-MASK | any | host DESTINATION ) ( dst-port OPERATOR PORT | ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( established | ( match-any | match-all FLAG-NAME | ) | ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment ) ( routed-packet | ) ( options | ) ( time-range TIME-RANGE-NAME | )
```

Please reference to command “deny tcp” for the parameters.

Command Mode

IP ACL configuration

Default

None

Usage

The fragments will be invalid when the layer 4 information is specified (i.e. src-port).

Examples

This example shows how to create a filter in IP ACL to permit any TCP packets.

```
Switch(config-ip-acl)# 10 permit tcp any any
```

This example shows how to create a filter in IP ACL to permit the TCP packets with the source IP address 1.1.1.1, and source port ranges from 0 to 100.

```
Switch(config-ip-acl)# 20 permit tcp host 1.1.1.1 src-port range 0 100 any
```

This example shows how to create a filter in IP ACL to permit any TCP packets in established TCP streams.

```
Switch(config-ip-acl)# 30 permit tcp any any established
```

This example shows how to create a filter in IP ACL to permit the TCP ACK packets with the source IP address 10.10.10.0.

```
Switch(config-ip-acl)# 4 permit tcp 10.10.10.0 0.0.0.0 any match-any ack
```

Related Commands

no sequence-num

4.15 permit udp

Use this command to permit UDP packets when the packets match this access-list.

Command Syntax

```
(SEQUENCE-NUM | ) permit udp ( source SOURCE-MASK | any | host SOURCE )  
( src-port OPERATOR PORT | )( destination DESTINATION-MASK | any | host  
DESTINATION ) ( dst-port OPERATOR PORT | ) ( ip-precedence PRECEDENCE | dscp  
DSCP | )  
( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-frag  
ment ) ( routed-packet | ) ( options | ) ( time-range TIME-RANGE-NAME | )
```

Please reference to command “deny udp” for the parameters.

Command Mode

IP ACL Configuration

Default

None

Usage

The fragments will be invalid when the layer 4 information is specified (i.e. src-port).

Examples

This example shows how to create a filter in IP ACL to deny any UDP packets.

```
Switch(config-ip-acl)# 1 permit udp any any
```

This example shows how to create a filter in IP ACL to deny the UDP packets with the source IP address 1.1.1.1, source port 10, and destination port less than 2000.

```
Switch(config-ip-acl)# 2 permit udp host 1.1.1.1 src-port eq 10 any dst-port lt 2000
```

Related Commands

no sequence-num

4.16 permit icmp

Use this command to permit ICMP packets matching the IP filter.

Command Syntax

```
(SEQUENCE-NUM | ) permit icmp ( source SOURCE-MASK | any | host SOURCE )  
( destination DESTINATION-MASK | any | host DESTINATION ) ( icmp-type TYPE-NUM  
( icmp-code CODE-NUM | ) | ) ( ip-precedence PRECEDENCE | dscp DSCP | )  
( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-frag  
ment ) ( routed-packet | ) ( options | ) ( time-range TIME-RANGE-NAME | )
```

Please reference to command “deny icmp” for the parameters.

Command Mode

IP ACL Configuration

Default

None

Usage

This type of filter is mostly used to permit ICMP packets.

Examples

This example shows how to create a filter in IP ACL to permit any ICMP packets.

```
Switch(config-ip-acl)# 1 permit icmp any any
```

This example shows how to create a filter in IP ACL to permit the ICMP packets with the icmp-type 3 and icmp-code 3.

```
Switch(config-ip-acl)# 2 permit icmp any any icmp-type 3 icmp-code 3
```

Related Commands

deny icmp

no sequence-num

4.17 permit igmp

Use this command to permit IGMP packets matching the IP filter.

Command Syntax

```
(SEQUENCE-NUM | ) permit igmp ( SOURCE SOURCE-MASK | any | host SOURCE )  
( DESTINATION DESTINATION-MASK | any | host DESTINATION ) ( IGMP-TYPE | )  
( ip-precedence PRECEDENCE | dscp DSCP | )  
( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment ) ( routed-packet | ) ( options | ) ( time-range TIME-RANGE-NAME | )
```

Please reference to command “deny igmp” for the parameters.

Command Mode

IP ACL Configuration

Default

None

Usage

This type of filter is mostly used to permit IGMP packets.

Examples

This example shows how to create a filter in IP ACL to permit any IGMP packets.

```
Switch(config-ip-acl)# 1 permit igmp any any
```

This example shows how to create a filter in IP ACL to permit the IGMP packets with the source IP address 1.1.1.1, any destination IP address and the igmp-type pim.

```
Switch(config-ip-acl)# 2 permit igmp host 1.1.1.1 any pim
```

Related Commands

no sequence-num

4.18 show access-list ip

Use this command to show the information of IP ACL.

Command Syntax

show access-list ip (*ACL-NAME* |)

<i>ACL-NAME</i>	The name of the IP ACL
-----------------	------------------------

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to show the information of IP ACL.

Switch# show access-list ip

```
ip access-list list_ipv4_1
 2 permit tcp host 1.1.1.1 any
 3 deny icmp any any
12 permit tcp any any
```

Related Commands

ip access-list

5

Extend ACL Commands

5.1 ip access-list extend

Use this command to create extend IP ACL and then enter extend IP ACL configuration mode.

To remove this ACL, use the no form of this command.

Command Syntax

ip access-list *ACL-NAME* **extend**

no ip access-list *ACL-NAME* **extend**

<i>ACL-NAME</i> extend	The name of an extend IP ACL
-------------------------------	------------------------------

Command Mode

Global Configuration

Default

None

Usage

If the system already has an extend IP ACL with the same name, this command will enter the extend IP ACL configuration mode. However, if the ACL name is used by other type of ACL, a prompt message will be shown.

When the name is not used by any ACL, this command is to create an extend IP ACL firstly and then enter the extend IP ACL configuration mode.

On how to apply the created extend IP ACL in the interface, please refer to the usage of match access-group command in related chapter.

Examples

This example shows how to create an extend IP ACL named list_ipv4_1 and then enter the extend IP ACL configuration mode.

```
Switch(config)# ip access-list list_ipv4_1 extend
Switch(config-ex-ip-acl1)#
```

This example shows how to remove the extend IP ACL named list_ipv4_1.

```
Switch(config)# no ip access-list list_ipv4_1 extend
```

Related Commands

match access-group

5.2 sequence-num

Use this command to delete a filter from extend IP ACL.

Command Syntax

no sequence-num *SEQUENCE-NUM*

<i>SEQUENCE-NUM</i>	The sequence number of an IP filter, the range is 1 to 131071
---------------------	---

Command Mode

Extend IP ACL configuration

Default

None

Usage

None

Examples

This example shows how to delete an IP or MAC filter with sequence number 10 from an extend IP ACL.

```
Switch(config-ex-ip-acl)# no sequence-num 10
```

Related Commands

deny
deny tcp
deny udp
deny icmp
deny igmp
permit
permit tcp
permit udp
permit icmp
permit igmp
deny src-mac
permit src-mac

5.3 deny src-mac

Use this command to create a filter for discarding ongoing packets matching the filter rule.

Command Syntax

(SEQUENCE-NUM |) **deny src-mac** (**any** | *MAC MASK* | **host** *MAC*) (**dest-mac** (**any** | *MAC MASK* | **host** *MAC*) |) (**vlan** *VLAN* |) (**cos** *VLAN* |) (**inner-vlan** *VLAN* |) (**inner-cos**

VALUE |) (**arp-packet** ((**arp-op-code**) (**sender-ip** (IP MASK|any|host IP|)) (**target-ip** (IP MASK|any|host IP|)))) (**time-range** *TIME-RANGE-NAME* |)

<i>SEQUENCE-NUM</i>	The sequence number of the filter in MAC ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented, The range is 1 to 131071
any	Any host
<i>MAC MASK</i>	The MAC address and its wildcard bits
host MAC	The host with a specified MAC address
dest-mac	Destination MAC address
vlan VLAN	VLAN-ID, the range is 1 to 4094
cos VALUE	CoS, the range is 0 to 7
inner-vlan VLAN	Inner VLAN-ID, the range is 1 to 4094
inner-cos VALUE	Inner CoS, the range is 0 to 7
arp	ARP protocol
arp-op-code	arp-op-code, the range is 0~65535
sender-ip	sender-ip
IP MASK	The sender ip address and its wildcard bits
any	Any sender ip
host IP	The host with a specified sender ip address
target-ip	target-ip
IP MASK	The target ip address and its wildcard bits
any	Any target ip
host IP	The host with a specified target ip address
time-range <i>TIME-RANGE-NAME</i>	The time-range used by the MAC filter

Command Mode

Extend IP ACL configuration

Default

None

Usage

An auto-generated sequence number will be assigned to the filter if the sequence-num field is not presented. The auto-generated sequence number is incremented by 10 on the maximum existing sequence number in the extend IP ACL. i.e. when the maximum existing sequence number is 100, the sequence number of subsequent created MAC filter is 110.

Examples

This example shows how to create a filter in extend IP ACL to deny the packets with source MAC address 001A.A02C.A1DF.

```
Switch(config-ex-ip-acl)# 1 deny src-mac host 001A.A02C.A1DF
```

This example shows how to create a filter in extend IP ACL to deny all the packets.

```
Switch(config-ex-ip-acl)# 2 deny src-mac any
```

This example shows how to create a filter in extend IP ACL to deny the packet whose source MAC address is between the ranges specified.

```
Switch(config-ex-ip-acl)# 3 deny src-mac 001A.A02C.A1DF 001A.A02C.0000
```

Related Commands

no sequence-num

5.4 permit src-mac

Use this command to create a filter for allowing packets matching the filter rule to be delivered.

Command Syntax

```
(SEQUENCE-NUM | ) permit src-mac (any | MAC MASK | host MAC) ( dest-mac (any | MAC MASK | host MAC) | ) ( vlan VLAN | ) ( cos VALUE | ) ( inner-vlan VLAN | ) ( inner-cos VALUE | ) (arp-packet ((arp-op-code) (sender-ip (IP MASK|any|host IP)|) (target-ip (IP MASK|any|host IP)|))) ( time-range TIME-RANGE-NAME | )
```

Please reference to command “deny src-mac” for the parameters.

Command Mode

Extend IP ACL configuration

Default

None

Usage

An auto-generated sequence number will be assigned to the filter if the sequence-num field is not presented. The auto-generated sequence number is incremented by 10 on the maximum existing sequence number in the extend IP ACL. i.e. when the maximum existing sequence number is 105, the sequence number of subsequent created MAC filter is 115.

Examples

This example shows how to create a filter in extend IP ACL to permit the packets with source MAC address 001A.A02C.A1DF.

```
Switch(config-ex-ip-acl)# 1 permit src-mac host 001A.A02C.A1DF
```

This example shows how to create a filter in extend IP ACL to permit all the packets.

```
Switch(config-ex-ip-acl)# 2 permit src-mac any
```

This example shows how to create a filter in MAC ACL to permit the packets with source MAC address between the ranges specified.

```
Switch(config-ex-ip-acl)# 3 permit src-mac 001A.A02C.A1DF 001A.A02C.0000
```

Related Commands

no sequence-num

5.5 deny

Use this command to discard ongoing IP packets matching the IP filter.

Command Syntax

```
(SEQUENCE-NUM | ) deny (PROTO-NUM | any) ( SOURCE SOURCE-MASK | any | host
SOURCE) (DESTINATION DESTINATION-MASK | any | host DESTINATION)
( ip-precedence PRECEDENCE | dscp DSCP | )
(non-fragment|first-fragment|non-or-first-fragment|small-fragment|non-first-frag
ment) ( routed-packet | ) ( options | ) ( time-range TIME-RANGE-NAME | )
```

<i>SEQUENCE-NUM</i>	The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented. The range is 1 to 131071
<i>PROTO-NUM</i>	An IP protocol number, the range is 0 to 255
any	Any IP protocol
<i>SOURCE SOURCE-MASK</i>	The source IP address and its wildcard bits
any	Any source host
host <i>SOURCE</i>	The source IP address of a host
<i>DESTINATION DESTINATION-MASK</i>	The destination IP address and its wildcard bits
any	Any destination host
host <i>DESTINATION</i>	The destination IP address of a host
ip-precedence <i>PRECEDENCE</i>	Match packets with given precedence value, the range is 0 to 7
dscp <i>DSCP</i>	Match packets with given dscp value, the range is 0 to 63
non-fragment	Match packets with non fragment
first-fragment	Match packets with first fragment
non-or-first-fragment	Match packets with non first fragment
small-fragment	Match packets with small fragment
non-first-fragment	Match packets with non first fragment
routed-packet	Match routed packet
options	Match packets with IP options
time-range <i>TIME-RANGE-NAME</i>	The time-range used by the IP filter

Command Mode

Extend IP ACL configuration

Default

None

Usage

If an IP address wildcard bit is provided, the IP address is logically-anded in bitwise with the reverse bits of the wildcard bits. For example, 10.10.10.0 0.0.0.255 means the addresses from 10.10.10.0 to 10.10.10.255 are matched.

An auto-generated sequence number will be assigned to the filter if the sequence-num field is not presented. The auto-generated sequence number is incremented by 10 on the maximum existing sequence number in the extend IP ACL. i.e. when the maximum existing sequence number is 100, the sequence number of subsequent created IP filter is 110.

Examples

This example shows how to create a filter in extend IP ACL to deny any IP packets.

```
Switch(config-ex-ip-acl)# 1 deny any any any
```

This example shows how to create a filter in extend IP ACL to deny the fragment packets with the source IP addresses 1.1.1.1.

```
Switch(config-ex-ip-acl)# 2 deny any host 1.1.1.1 any fragments
```

This example shows how to create a filter in extend IP ACL to deny any routed packets.

```
Switch(config-ex-ip-acl)# 3 deny any any any routed-packet
```

Related Commands

no sequence-num

5.6 deny tcp

Use this command to reject TCP packets matching the IP filter.

Command Syntax

```
(SEQUENCE-NUM | ) deny tcp ( SOURCE SOURCE-MASK | any | host SOURCE ) ( src-port OPERATOR PORT | )( DESTINATION DESTINATION-MASK | any | host DESTINATION ) ( dst-port OPERATOR PORT | ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( established | ( match-any | match-all FLAG-NAME | ) | ) ( non-fragment | first-fragment | non-or-first-fragment | small-fragment | non-first-fragment ) ( routed-packet | ) ( options | ) ( time-range TIME-RANGE-NAME | )
```

<i>SEQUENCE-NUM</i>	The sequence number of the filter in IP ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented. The range is 1 to 2147483646
<i>SOURCE SOURCE-MASK</i> k	The source IP address and its wildcard bits
any	Any source host
host <i>SOURCE</i>	The source IP address of a host
src-port <i>OPERATOR PORT</i>	Source port, the range is 0 to 65535. Including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range
<i>DESTINATION DESTINATION-MASK</i>	The destination IP address and its wildcard bits
any	Any destination host

host <i>DESTINATION</i>	The destination IP address of a host
dst-port <i>OPERATOR PORT</i>	Destination port, the range is 0 to 65535. Including eq (equal to), lt (less than), gt (greater than), neq (not equal to) and range
ip-precedence <i>PRECEDENCE</i>	Match packets with given precedence value, the range is 0 to 7
dscp <i>DSCP</i>	Match packets with given dscp value, the range is 0 to 63
established	Match established connections
match-any	Match any of the flag-name
match-all <i>FLAG-NAME</i>	Match all the flag-name, including ack, fin, psh, rst, syn and urg
non-fragment	Match packets with non fragment
first-fragment	Match packets with first fragment
non-or-first-fragment	Match packets with non first fragment
small-fragment	Match packets with small fragment
non-first-fragment	Match packets with non first fragment
routed-packet	Match routed packet
options	Match packets with IP options
time-range <i>TIME-RANGE-NAME</i>	The time-range used by the IP filter

Command Mode

Extend IP ACL configuration

Default

None

Usage

The fragments will be invalid when the layer 4 information is specified (i.e. src-port).

Examples

This example shows how to create a filter in extend IP ACL to deny any TCP packets.

```
Switch(config-ex-ip-acl1)# 1 deny tcp any any
```

This example shows how to create a filter in extend IP ACL to deny the TCP packets with the source IP address 1.1.1.1, source port 0-100.

```
Switch(config-ex-ip-acl1)# 2 deny tcp host 1.1.1.1 src-port range 0 100 any
```

This example shows how to create a filter in extend IP ACL to deny any TCP packets in established TCP streams.

```
Switch(config-ex-ip-acl1)# 3 deny tcp any any established
```

This example shows how to create a filter in extend IP ACL to deny the TCP ACK packets with the source IP address 1.1.1.1.

```
Switch(config-ex-ip-acl1)# 4 deny tcp 10.10.10.0 0.0.0.0 any match-any ack
```

Related Commands

no sequence-num

5.7 deny udp

Use this command to reject UDP packets matching the IP filter.

Command Syntax

```
(SEQUENCE-NUM | ) deny udp ( SOURCE SOURCE-MASK | any | host SOURCE ) ( src-port OPERATOR PORT | )(DESTINATION DESTINATION-MASK | any | host DESTINATION) ( dst-port OPERATOR PORT | ) ( ip-precedence PRECEDENCE | dscp DSCP | ) (non-fragment|first-fragment|non-or-first-fragment|small-fragment|non-first-fragment) ( routed-packet | ) ( options | ) ( time-range TIME-RANGE-NAME | )
```

Please reference to “deny tcp” for the parameters.

Command Mode

Extend IP ACL configuration

Default

None

Usage

The fragments will be invalid when the layer 4 information is specified (i.e. src-port).

Examples

This example shows how to create a filter in extend IP ACL to deny any UDP packets.

```
Switch(config-ex-ip-acl)# 1 deny udp any any
```

This example shows how to create a filter in extend IP ACL to deny the UDP packets with the source IP 1.1.1.1, source port 10, and destination port less than 2000.

```
Switch(config-ex-ip-acl)# 2 deny udp host 1.1.1.1 src-port eq 10 any dst-port lt 2000
```

Related Commands

no sequence-num

5.8 deny icmp

Use this command to reject ICMP packets matching the IP filter.

Command Syntax

```
(SEQUENCE-NUM | ) deny icmp ( SOURCE SOURCE-MASK | any | host SOURCE ) (DESTINATION DESTINATION-MASK | any | host DESTINATION) ( icmp-type TYPE-NUM ( icmp-code CODE-NUM | ) | ) ( ip-precedence PRECEDENCE | dscp DSCP | ) (non-fragment|first-fragment|non-or-first-fragment|small-fragment|non-first-fragment) ( routed-packet | ) ( options | ) ( time-range TIME-RANGE-NAME | )
```

icmp-type TYPE-NUM	ICMP message type, the range is 0 to 255
icmp-code CODE-NUM	ICMP message code, the range is 0 to 255

Please reference to “deny” for the parameters.

Command Mode

Extend IP ACL configuration

Default

None

Usage

None

Examples

This example shows how to create a filter in extend IP ACL to deny any ICMP packets.

```
Switch(config-ex-ip-acl1)# 1 deny icmp any any
```

This example shows how to create a filter in extend IP ACL to deny the ICMP packets with the icmp-type 3 and icmp-code 3.

```
Switch(config-ex-ip-acl1)# 2 deny icmp any any icmp-type 3 icmp-code 3
```

Related Commands

no sequence-num

5.9 deny igmp

Use this command to reject IGMP packets matching the IP filter.

Command Syntax

(SEQUENCE-NUM |) **deny igmp** (*SOURCE SOURCE-MASK | any | host SOURCE*)
 (*DESTINATION DESTINATION-MASK | any | host DESTINATION*) (*IGMP-TYPE |*)
 (**ip-precedence** *PRECEDENCE* | **dscp** *DSCP* |)
 (**non-fragment|first-fragment|non-or-first-fragment|small-fragment|non-first-fragment**) (**routed-packet** |) (**options** |) (**time-range** *TIME-RANGE-NAME* |)

<i>IGMP-TYPE</i>	IGMP type, including dvmrp, host-query, host-report, mtrace, mtrace-response, pim, precedence, trace, v2-leave, v2-report, v3-report
------------------	--

Please reference to “deny” for the parameters.

Command Mode

Extend IP ACL configuration

Default

None

Usage

None

Examples

This example shows how to create a filter in extend IP ACL to deny any IGMP packets.

```
Switch(config-ex-ip-acl1)# 1 deny igmp any any
```

This example shows how to create a filter in extend IP ACL to deny the IGMP packets with the source IP address 1.1.1.1, any destination IP address and the igmp-type pim.

```
Switch(config-ex-ip-acl1)# 2 deny igmp host 1.1.1.1 any pim
```

Related Commands

no sequence-num

5.10 permit

Use this command to permit packets matching the IP filter.

Command Syntax

```
(SEQUENCE-NUM | ) permit (PROTO-NUM | any) ( source SOURCE-MASK | any | host SOURCE ) (destination DESTINATION-MASK | any | host DESTINATION )  
( ip-precedence PRECEDENCE | dscp DSCP | )  
(non-fragment|first-fragment|non-or-first-fragment|small-fragment|non-first-fragment) ( routed-packet | ) ( options | ) ( time-range TIME-RANGE-NAME | )
```

Please reference to “deny” for the parameters.

Command Mode

Extend IP ACL configuration

Default

None

Usage

If an IP address wildcard bit is provided, the IP address is logically-anded in bitwise with the reverse bits of the wildcard bits. For example, 10.10.10.0 0.0.0.255 means the addresses from 10.10.10.0 to 10.10.10.255 are matched.

An auto-generated sequence number will be assigned to the filter if the sequence-num field is not presented. The auto-generated sequence number is incremented by 10 on the maximum existing sequence number in the extend IP ACL. i.e. when the maximum existing sequence number is 105, the sequence number of subsequent created IP filter is 115.

Examples

This example shows how to create a filter in extend IP ACL to permit any IP packets.

```
Switch(config-ex-ip-acl1)# 10 permit any any any
```

This example shows how to create a filter in extend IP ACL to permit the fragment packets with the source IP address 1.1.1.1 and any destination IP address.

```
Switch(config-ex-ip-acl1)# 20 permit tcp host 1.1.1.1 any fragments
```

This example shows how to create a filter in extend IP ACL to permit any routed packets.

```
Switch(config-ex-ip-acl1)# 30 permit any any any routed-packet
```

Related Commands

no sequence-num

5.11 permit tcp

Use this command to permit TCP packets matching the IP filter.

Command Syntax

```
(SEQUENCE-NUM | ) permit tcp (source SOURCE-MASK | any | host SOURCE )( src-port OPERATOR PORT | )(DESTINATION DESTINATION-MASK | any | host DESTINATION) ( dst-port OPERATOR PORT | ) ( ip-precedence PRECEDENCE | dscp DSCP | ) ( established | ( match-any | match-all FLAG-NAME | ) | ) (non-fragment|first-fragment|non-or-first-fragment|small-fragment|non-first-fragment) ( routed-packet | ) ( options | ) ( time-range TIME-RANGE-NAME | )
```

Please reference to “deny tcp” for the parameters.

Command Mode

Extend IP ACL configuration

Default

None

Usage

The fragments will be invalid when the layer 4 information is specified (i.e. src-port).

Examples

This example shows how to create a filter in extend IP ACL to permit any TCP packets.

```
Switch(config-ex-ip-acl)# 10 permit tcp any any
```

This example shows how to create a filter in extend IP ACL to permit the TCP packets with the source IP address 1.1.1.1, and source port ranges from 0 to 100.

```
Switch(config-ex-ip-acl)# 20 permit tcp host 1.1.1.1 src-port range 0 100 any
```

This example shows how to create a filter in extend IP ACL to permit any TCP packets in established TCP streams.

```
Switch(config-ex-ip-acl)# 30 permit tcp any any established
```

This example shows how to create a filter in extend IP ACL to permit the TCP ACK packets with the source IP address 10.10.10.0.

```
Switch(config-ex-ip-acl)# 4 permit tcp 10.10.10.0 0.0.0.0 any match-any ack
```

Related Commands

no sequence-num

5.12 permit udp

Use this command to permit UDP packets when the packets match this access-list.

Command Syntax

```
(SEQUENCE-NUM | ) permit udp ( source SOURCE-MASK | any | host SOURCE ) ( src-port OPERATOR PORT | )(destination DESTINATION-MASK | any | host DESTINATION) ( dst-port OPERATOR PORT | ) ( ip-precedence PRECEDENCE | dscp DSCP | ) (non-fragment|first-fragment|non-or-first-fragment|small-fragment|non-first-fragment) ( routed-packet | ) ( options | ) ( time-range TIME-RANGE-NAME | )
```

Please reference to “deny udp” for the parameters.

Command Mode

Extend IP ACL configuration

Default

None

Usage

The fragments will be invalid when the layer 4 information is specified (i.e. src-port).

Examples

This example shows how to create a filter in extend IP ACL to deny any UDP packets.

```
Switch(config-ex-ip-acl1)# 1 permit udp any any
```

This example shows how to create a filter in extend IP ACL to deny the UDP packets with the source IP address 1.1.1.1, source port 10, and destination port less than 2000

```
Switch(config-ex-ip-acl1)# 2 permit udp host 1.1.1.1 src-port eq 10 any dst-port lt 2000
```

Related Commands

no sequence-num

5.13 permit icmp

Use this command to permit ICMP packets when the packets match this access-list.

Command Syntax

```
(SEQUENCE-NUM | ) permit icmp (source SOURCE-MASK | any | host SOURCE )  
(destination DESTINATION-MASK | any | host DESTINATION ) ( icmp-type TYPE-NUM  
( icmp-code CODE-NUM | ) | ) ( ip-precedence PRECEDENCE | dscp DSCP | )  
(non-fragment|first-fragment|non-or-first-fragment|small-fragment|non-first-frag  
ment) ( routed-packet | ) ( options | ) ( time-range TIME-RANGE-NAME | )
```

Please reference to “deny icmp” for the parameters.

Command Mode

Extend IP ACL configuration

Default

None

Usage

None

Examples

This example shows how to create a filter in extend IP ACL to permit any ICMP packets.

```
Switch(config-ex-ip-acl1)# 1 permit icmp any any
```

This example shows how to create a filter in extend IP ACL to permit the ICMP packets with the icmp-type 3 and icmp-code 3.

```
Switch(config-ex-ip-acl1)# 2 permit icmp any any icmp-type 3 icmp-code 3
```

Related Commands

None

5.14 permit igmp

Use this command to permit IGMP packets matching the IP filter.

Command Syntax

(*SEQUENCE-NUM* |) **permit igmp** (*SOURCE SOURCE-MASK* | **any** | **host** *SOURCE*)
 (*DESTINATION DESTINATION-MASK* | **any** | **host** *DESTINATION*) (*IGMP-TYPE* |)
 (**ip-precedence** *PRECEDENCE* | **dscp** *DSCP* |)
 (**non-fragment**|**first-fragment**|**non-or-first-fragment**|**small-fragment**|**non-first-frag**
ment) (**routed-packet** |) (**options** |) (**time-range** *TIME-RANGE-NAME* |)

Please reference to “deny igmp” for the parameters.

Command Mode

Extend IP ACL configuration

Default

None

Usage

None

Examples

This example shows how to create a filter in extend IP ACL to permit any IGMP packets.

```
Switch(config-ex-ip-acl1)# 1 permit igmp any any
```

This example shows how to create a filter in extend IP ACL to permit the IGMP packets with the source IP address 1.1.1.1, any destination IP address and the igmp-type pim.

```
Switch(config-ex-ip-acl1)# 2 permit igmp host 1.1.1.1 any pim
```

Related Commands

no sequence-num

5.15 remark

Use this command to add remarks for the extend IP ACL.

To remove remarks from the extend IP ACL, use the no form of this command.

Command Syntax

remark *REMARK*

no remark

<i>REMARK</i>	The remarks of the extend IP ACL
---------------	----------------------------------

Command Mode

Extend IP ACL configuration

Default

None

Usage

The remark is up to 100 characters.

Examples

This example shows how to add a remark to describe the extend IP ACL.

```
Switch(config-ex-ip-acl1)# remark remard0flist1
```

This example shows how to remove the remark from the extend IP ACL.

```
Switch(config-ex-ip-acl1)# no remark
```

Related Commands

None

5.16 show access-list ip

Use this command to show the information of extend IP ACL.

Command Syntax

show access-list ip (*ACL-NAME* **extend** |)

<i>ACL-NAME</i> extend	The name of the extend IP ACL
------------------------	-------------------------------

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

This example shows how to show the information of extend IP ACL.

```
Switch# show access-list ip
ip access-list ex_ip_list_ipv4_1 extend
 2 permit tcp host 1.1.1.1 any
 3 deny icmp any any
12 permit tcp any any
```

Related Commands

ip access-list extend

6 ACLv6 Commands

6.1 ipv6 access-list

Use this command to create IPv6 ACL and then enter IPv6 ACL in global configuration mode.

Command Syntax

ipv6 access-list *ACL-NAME*

no ipv6 access-list *ACL-NAME*

<i>ACL-NAME</i>	The name of the IPv6 ACL
-----------------	--------------------------

Command Mode

Global Configuration

Default

None

Usage

If the system already has an IPv6 ACL with the same name, this command will enter the IPv6 ACL configuration mode. However, if the ACL name is used by other type of ACL, a prompt message will be shown.

When the name is not used by any ACL, this command is to create the IPv6 ACL firstly and then enter the IPv6 ACL configuration mode.

Examples

This example shows how to create an IPv6 ACL named list_ipv6_1 and then enter the IPv6 ACL configuration mode.

```
Switch(config)# ipv6 access-list list_ipv6_1
Switch(config-ipv6-acl)#
```

This example shows how to remove the IPv6 ACL named list_ipv6_1.

```
Switch(config)# no ipv6 access-list list_ipv6_1
```

Related Commands

match access-group

6.2 sequence-num

Use this command to remove a filter from IPv6 ACL.

Command Syntax

no sequence-num *SEQUENCE-NUM*

<i>SEQUENCE-NUM</i>	The sequence number of a IPv6 filter, the range is 1 to 131071
---------------------	--

Command Mode

IPv6 ACL Configuration

Default

None

Usage

None

Examples

This example shows how to remove a filter with the sequence-num 10 from IPv6 ACL.

```
Switch(config-ipv6-acl)# no sequence-num 10
```

Related Commands

deny

deny tcp

deny udp

deny icmp

permit

permit tcp

permit udp

permit icmp

6.3 remark

Use this command to add remarks for the IPv6 ACL.

To remove remarks of the IPv6 ACL, use the no form of this command.

Command Syntax

remark *REMARK*

no remark

<i>REMARK</i>	The remarks of the IPv6 ACL
---------------	-----------------------------

Command Mode

IPv6 ACL Configuration

Default

None

Usage

The remarks are up to 100 characters. The exceed parts will not be stored and will be truncated.

Examples

This example shows how to add a remark to describe the IPv6 ACL.

```
Switch(config-ipv6-acl)# remark remark of List for ipv6
```

This example shows how to remove the remark of the IPv6 ACL.

```
Switch(config-ipv6-acl)# no remark
```

Related Commands

ipv6 access-list

6.4 show access-list ipv6

Use this command to show the IPv6 ACL information.

Command Syntax

show access-list ipv6 (*ACL-NAME* |)

<i>ACL-NAME</i>	The name of the IPv6 ACL
-----------------	--------------------------

Command Mode

Privileged EXEC

Default

None

Usage

If no ipv6 acl are specified, all ipv6 access-lists in the system should be shown.

Examples

This example shows how to show the IPv6 ACL information.

```
Switch# show access-list ipv6
ipv6 access-list list_ipv6_1
 10 deny any 2001::/48 any
 20 permit any any any
```

Related Commands

ipv6 access-list

6.5 deny

Use this command to discard ongoing IPv6 packets matching the IPv6 filter.

Command Syntax

(*SEQUENCE-NUM* |) **deny** (*PROTO-NUM* | **any**) (*SOURCE-PREFIX* | **any** | **host** *SOURCE*) (*DESTINATION-PREFIX* | **any** | **host** *DESTINATION*) (**routed-packet** |) (**time-range** *TIME-RANGE-NAME* |)

<i>SEQUENCE-NUM</i>	The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented. The range is 1 to 131071
<i>PROTO-NUM</i>	An IPv6 protocol number, the range is 0 to 255
any	Any IPv6 protocol
<i>SOURCE-PREFIX</i>	The source IPv6 prefix address
any	Any source host
host <i>SOURCE</i>	The source IPv6 address of a host
<i>DESTINATION-PREFIX</i>	The destination IPv6 prefix address
any	Any destination host
host <i>DESTINATION</i>	The destination IPv6 address of a host
routed-packet	Match routed packet
time-range <i>TIME-RANGE-NAME</i>	The time-range used by the IPv6 filter

Command Mode

IPv6 ACL configuration

Default

None

Usage

An auto-generated sequence number will be assigned to the filter if the sequence-num field is not presented. The auto-generated sequence number is incremented by 10 on the maximum existing sequence number in the IPv6 ACL. For example, when the maximum existing sequence number is 100, the sequence number of subsequent created IPv6 filter is 110.

Examples

This example shows how to create a filter in IPv6 ACL to deny any IPv6 packets.

```
Switch(config-ipv6-acl)# 1 deny any any any
```

This example shows how to create a filter in IPv6 ACL to deny any routed packets.

```
Switch(config-ipv6-acl)# 2 deny any any any routed-packet
```

Related Commands

no sequence-num

6.6 deny tcp

Use this command to reject TCP packets matching the IPv6 filter.

Command Syntax

(SEQUENCE-NUM |) deny tcp (SOURCE-PREFIX | any | host SOURCE) (src-port OPERATOR PORT |) (DESTINATION-PREFIX | any | host DESTINATION) (dst-port OPERATOR PORT |) (routed-packet |) (time-range TIME-RANGE-NAME |)

<i>SEQUENCE-NUM</i>	The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented. the range is 1 to 131071
<i>SOURCE-PREFIX</i>	The source IPv6 prefix address
any	Any source host
host SOURCE	The source IPv6 address of a host
src-port OPERATOR PORT	Source port, the range is 0 to 65535, including eq (equal to)
<i>DESTINATION-PREFIX</i>	The destination IPv6 prefix address
any	Any destination host
host DESTINATION	The destination IPv6 address of a host
dst-port OPERATOR PORT	Destination port, the range is 0 to 65535, including eq (equal to)
routed-packet	Match routed packet
time-range TIME-RANGE-NAME	The time-range used by the IPv6 filter

Command Mode

IPv6 ACL configuration

Default

None

Usage

None

Examples

This example shows how to create a filter in IPv6 ACL to deny any TCP packets.

```
Switch(config-ipv6-acl)# 1 deny tcp any any
```

This example shows how to create a filter in IPv6 ACL to deny the TCP packets with the source IPv6 address 2001::2020, source port 8080.

```
Switch(config-ipv6-acl)# 2 deny tcp host 2001::2020 src-port eq 8080 any
```

Related Commands

no sequence-num

6.7 deny udp

Use this command to reject UDP packets matching the IPv6 filter.

Command Syntax

(*SEQUENCE-NUM* |) **deny udp** (*SOURCE-PREFIX* | **any** | **host** *SOURCE*) (**src-port** *OPERATOR PORT* |) (*DESTINATION-PREFIX* | **any** | **host** *DESTINATION*) (**dst-port** *OPERATOR PORT* |) (**routed-packet** |) (**time-range** *TIME-RANGE-NAME* |)

Please reference to command “deny tcp” for the parameters.

Command Mode

IPv6 ACL configuration

Default

None

Usage

None

Examples

This example shows how to create a filter in IPv6 ACL to deny any UDP packets.

```
Switch(config-ipv6-acl)# 1 deny udp any any
```

This example shows how to create a filter in IPv6 ACL to deny the UDP packets with the source IPv6 address 2001::2020, source port 8080.

```
Switch(config-ipv6-acl)# 2 deny udp host 2001::2020 src-port eq 8080 any
```

Related Commands

no sequence-num

6.8 deny icmp

Use this command to reject ICMP packets matching the IPv6 filter.

Command Syntax

(*SEQUENCE-NUM* |) **deny icmp** (*SOURCE-PREFIX* | **any** | **host** *SOURCE*) (*DESTINATION-PREFIX* | **any** | **host** *DESTINATION*) (**icmp-type** *TYPE-NUM* (**icmp-code** *CODE-NUM* |)) (**routed-packet** |) (**time-range** *TIME-RANGE-NAME* |)

icmp-type <i>TYPE-NUM</i>	ICMP message type, the range is 0 to 255
icmp-code <i>CODE-NUM</i>	ICMP message code, the range is 0 to 255

Please reference to command “deny” for the parameters.

Command Mode

IPv6 ACL configuration

Default

None

Usage

None

Examples

This example shows how to create a filter in IPv6 ACL to deny any ICMP packets.

```
Switch(config-ipv6-acl)# 1 deny icmp any any
```

This example shows how to create a filter in IPv6 ACL to deny the ICMP packets with the icmp-type 3 and icmp-code 3.

```
Switch(config-ipv6-acl)# 2 deny icmp any any icmp-type 3 icmp-code 3
```

Related Commands

no sequence-num

6.9 permit

Use this command to permit ongoing IPv6 packets matching the IPv6 filter.

Command Syntax

(SEQUENCE-NUM |) **permit** (*PROTO-NUM | any*) (*SOURCE-PREFIX | any | host SOURCE*) (*DESTINATION-PREFIX | any | host DESTINATION*) (**routed-packet** |) (**time-range** *TIME-RANGE-NAME* |)

<i>SEQUENCE-NUM</i>	The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented. The range is 1 to 131071
<i>PROTO-NUM</i>	An IPv6 protocol number, the range is 0 to 255
any	Any IPv6 protocol
<i>SOURCE-PREFIX</i>	The source IPv6 prefix address
any	Any source host
host <i>SOURCE</i>	The source IPv6 address of a host
<i>DESTINATION-PREFIX</i>	The destination IPv6 prefix address
any	Any destination host
host <i>DESTINATION</i>	The destination IPv6 address of a host
routed-packet	Match routed packet
time-range <i>TIME-RANGE-NAME</i>	The time-range used by the IPv6 filter

Command Mode

IPv6 ACL configuration

Default

None

Usage

An auto-generated sequence number will be assigned to the filter if the sequence-num field is not presented. The auto-generated sequence number is incremented by 10 on the maximum existing sequence number in the IPv6 ACL. For example, when the maximum

existing sequence number is 100, the sequence number of subsequent created IPv6 filter is 110.

Examples

This example shows how to create a filter in IPv6 ACL to permit any IPv6 packets.

```
Switch(config-ipv6-acl)# 1 permit any any any
```

This example shows how to create a filter in IPv6 ACL to permit any routed packets.

```
Switch(config-ipv6-acl)# 2 permit any any any routed-packet
```

Related Commands

no sequence-num

6.10 permit tcp

Use this command to permit TCP packets matching the IPv6 filter.

Command Syntax

(SEQUENCE-NUM |) **permit tcp** (*SOURCE-PREFIX | any | host SOURCE*) (**src-port** *OPERATOR PORT* |) (*DESTINATION-PREFIX | any | host DESTINATION*) (**dst-port** *OPERATOR PORT* |) (**routed-packet** |) (**time-range** *TIME-RANGE-NAME* |)

<i>SEQUENCE-NUM</i>	The sequence number of the filter in IPv6 ACL. An auto-generated sequence number will be assigned to the filter if this field is not presented. the range is 1 to 131071
<i>SOURCE-PREFIX</i>	The source IPv6 prefix address
any	Any source host
host <i>SOURCE</i>	The source IPv6 address of a host
src-port <i>OPERATOR PORT</i>	Source port, the range is 0 to 65535, including eq (equal to)
<i>DESTINATION-PREFIX</i>	The destination IPv6 prefix address
any	Any destination host
host <i>DESTINATION</i>	The destination IPv6 address of a host
dst-port <i>OPERATOR PORT</i>	Destination port, the range is 0 to 65535, including eq (equal to)
routed-packet	Match routed packet
time-range <i>TIME-RANGE-NAME</i>	The time-range used by the IPv6 filter

Command Mode

IPv6 ACL configuration

Default

None

Usage

None

Examples

This example shows how to create a filter in IPv6 ACL to permit any TCP packets.

```
Switch(config-ipv6-acl)# 1 permit tcp any any
```

This example shows how to create a filter in IPv6 ACL to permit the TCP packets with the source IPv6 address 2001::2020, source port 8080.

```
Switch(config-ipv6-acl)# 2 permit tcp host 2001::2020 src-port eq 8080 any
```

Related Commands

no sequence-num

6.11 permit udp

Use this command to permit UDP packets matching the IPv6 filter.

Command Syntax

(*SEQUENCE-NUM* |) **permit udp** (*SOURCE-PREFIX* | **any** | **host** *SOURCE*) (**src-port** *OPERATOR PORT* |) (*DESTINATION-PREFIX* | **any** | **host** *DESTINATION*) (**dst-port** *OPERATOR PORT* |) (**routed-packet** |) (**time-range** *TIME-RANGE-NAME* |)

Please reference to command “permit tcp” for the parameters.

Command Mode

IPv6 ACL configuration

Default

None

Usage

None

Examples

This example shows how to create a filter in IPv6 ACL to permit any UDP packets.

```
Switch(config-ipv6-acl)# 1 permit udp any any
```

This example shows how to create a filter in IPv6 ACL to permit the UDP packets with the source IPv6 address 2001::2020, source port 8080.

```
Switch(config-ipv6-acl)# 2 permit udp host 2001::2020 src-port eq 8080 any
```

Related Commands

no sequence-num

6.12 permit icmp

Use this command to reject ICMP packets matching the IPv6 filter.

Command Syntax

(*SEQUENCE-NUM* |) **permit icmp** (*SOURCE-PREFIX* | **any** | **host** *SOURCE*) (*DESTINATION-PREFIX* | **any** | **host** *DESTINATION*) (**icmp-type** *TYPE-NUM* (**icmp-code** *CODE-NUM* |) |) (**routed-packet** |) (**time-range** *TIME-RANGE-NAME* |)

icmp-type	ICMP message type, the range is 0 to 255
------------------	--

<i>TYPE-NUM</i>	
icmp-code <i>CODE-NUM</i>	ICMP message code, the range is 0 to 255

Please reference to command “permit” for the parameters.

Command Mode

IPv6 ACL configuration

Default

None

Usage

None

Examples

This example shows how to create a filter in IPv6 ACL to permit any ICMP packets.

```
Switch(config-ipv6-acl)# 1 permit icmp any any
```

This example shows how to create a filter in IPv6 ACL to permit the ICMP packets with the icmp-type 3 and icmp-code 3.

```
Switch(config-ipv6-acl)# 2 permit icmp any any icmp-type 3 icmp-code 3
```

Related Commands

no sequence-num

7

IEEE 802.1x Commands

7.1 dot1x system-auth-ctrl

Use the dot1x system-auth-ctrl to globally start the dot1x authenticate control feature. To remove this configure, use no form of this command.

Command Syntax

dot1x system-auth-ctrl
no dot1x system-auth-ctrl

Command Mode

Global Configuration

Default

Disable

Usage

Use this command to globally start the dot1x feature. To make the dot1x configures on each port work normally, this command should be used.

Examples

The following is sample output from the dot1x system-auth-ctrl command:

```
Switch(config)# dot1x system-auth-ctrl  
Switch(config)# no dot1x system-auth-ctrl
```

Related Commands

show dot1x
dot1x port-control

7.2 dot1x initialize

Use the dot1x initialize privileged EXEC command on the switch to manually return the specified IEEE 802.1x-enabled port to an unauthorized state before initiating a new authentication session on the port.

Command Syntax

dot1x initialize interface *interface-name*

interface <i>interface-name</i>	Specify the interface name to be initialized
--	--

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to initialize the IEEE 802.1x state machines and to set up a fresh environment for authentication. After you enter this command, the port status becomes unauthorized.

Examples

The following is sample output from the dot1x initialize command:

```
Switch# dot1x initialize interface eth-0-1
```

Related Commands

show dot1x

7.3 dot1x max-reauth-req

Use the dot1x max-reauth-req interface configuration command on the switch to set the maximum number of times that the switch restarts the authentication process before a port changes to the unauthorized state. Use the no form of this command to return to the default setting.

Command Syntax

dot1x max-reauth-req *count*

no dot1x max-reauth-req

max-reauth-req <i>count</i>	Number of times that the switch restarts the authentication process before the port changes to the unauthorized state. The range is 1 to 10
---------------------------------------	---

Command Mode

Interface Configuration

Default

The default value of dot1x max-reauth-req is 2 times.

Usage

You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Examples

The following is sample output from the dot1x max-reauth-req command:

```
Switch(config-if)# dot1x max-reauth-req 4
```

Related Commands

show dot1x

7.4 dot1x port-control

Use the dot1x port-control interface configuration command on the switch to enable manual control of the authorization state of the port. Use the no form of this command to return to the default setting.

Support config dot1x in routed port, while can't config it in a logical port such as agg, and so on.

Command Syntax

dot1x port-control (auto | force-authorized | force-unauthorized | dir (both | in))
no dot1x port-control

auto	Enable IEEE 802.1x authentication on the port and cause the port to change to the authorized or unauthorized state based on the IEEE 802.1x authentication exchange between the switch and the client
force-authorized	Disable IEEE 802.1x authentication on the port and cause the port to transition to the authorized state without an authentication exchange. The port sends and receives normal traffic without IEEE 802.1x-based authentication of the client
force-unauthorized	Deny all access through this port by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the port
dir	Specify the dot1x control direction
both	Discard received and transmitted packets
in	Discard received packets only

Command Mode

Interface Configuration

Default

The default value of the control direction is "in".

Usage

You must globally enable IEEE 802.1x authentication on the switch by using the dot1x system-auth-control global configuration command before enabling IEEE 802.1x authentication on a specific port.

Examples

The following is sample output from the dot1x port-control command:

```
Switch(config-if)# dot1x port-control auto
```

Related Commands

show dot1x

7.5 dot1x protocol-version

Use the dot1x protocol-version interface configuration command on the switch to set the version of EAPOL packets. Use the no form of this command to return to the default setting.

Command Syntax

dot1x protocol-version *version*

no dot1x protocol-version

protocol-version <i>version</i>	The EAPOL version. Default is 2
---	---------------------------------

Command Mode

Interface Configuration

Default

The default value of EAPOL version is 2.

Usage

You must specify the control of the authorization state of the port by the dot1x port-control command, before setting the EAPOL version.

Examples

The following is sample output from the dot1x protocol-version command:

```
Switch(config-if) # dot1x protocol-version 1
```

Related Commands

show dot1x

7.6 dot1x quiet-period

Use the dot1x quiet-period interface configuration command on the switch to set the quiet time interval. Use the no form of this command to return to the default setting.

Command Syntax

dot1x quiet-period *seconds*

no dot1x quiet-period

quiet-period <i>seconds</i>	The time interval (in seconds) between the retrials of authentication. The range is 1 to 65535.
---------------------------------------	---

Command Mode

Interface Configuration

Default

The default value of dot1x quite-period is 60 seconds.

Usage

During the quiet period, the switch does not accept or initiate any authentication requests. If you want to provide a faster response time to the user, enter a number smaller than the default.

Examples

The following is sample output from the dot1x quiet-period command:

```
Switch(config-if) # dot1x quiet-period 100
```

Related Commands

show dot1x

7.7 dot1x reauthentication

Use the dot1x reauthentication interface configuration command on the switch to enable periodic re-authentication of the client. Use the no form of this command to return to the default setting.

Command Syntax

dot1x reauthentication

no dot1x reauthentication

Command Mode

Interface Configuration

Default

None

Usage

The default setting of dot1x re-authentication is disabled. when the re-authentication is disabled, the configuration of the re-authenticate timeout should not take effect.

Examples

The following is sample output from the dot1x reauthentication command:

```
Switch(config-if) # dot1x reauthentication
```

Related Commands

show dot1x

dot1x timeout

7.8 dot1x re-authenticate

Use the dot1x re-authenticate privileged EXEC command on the switch stack to manually initiate a re-authentication of the specified IEEE 802.1x-enabled port.

Command Syntax

dot1x re-authenticate interface *interface-name*

interface <i>interface-name</i>	The interface to re-authenticate
--	----------------------------------

Command Mode

Privileged EXEC

Default

None

Usage

You can use this command to re-authenticate a client without waiting for the configured number of seconds between re-authentication attempts (re-authperiod) and automatic re-authentication.

Examples

The following is sample output from the dot1x re-authenticate command:

```
Switch# dot1x re-authenticate interface eth-0-1
```

Related Commands

show dot1x

7.9 dot1x timeout

Use the dot1x timeout interface configuration command on the switch stack or on a standalone switch to set IEEE 802.1x timers. Use the no form of this command to return to the default setting.

Command Syntax

dot1x timeout (re-authperiod *seconds* | server-timeout *seconds* | supp-timeout *seconds* | tx-period *seconds*)

no dot1x timeout (reauth-period | server-timeout | supp-timeout | tx-period)

re-authperiod <i>seconds</i>	Set the number of seconds between reauthentication attempts. The number of seconds from 1 to 65535
server-timeout <i>seconds</i>	Number of seconds that the switch waits for the retransmission of packets by the switch to the authentication server. The range is 1 to 65535
supp-timeout <i>seconds</i>	Number of seconds that the switch waits for the retransmission of packets by the switch to the IEEE 802.1x client. The range is 1 to 65535
tx-period <i>seconds</i>	Number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request. The range is 1 to 65535

Command Mode

Interface Configuration

Default

None

Usage

You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

The `dot1x timeout re-authperiod` interface configuration command affects the behavior of the switch only if you have enabled periodic re-authentication by using the `dot1x reauthentication` interface configuration command.

The default value of `re-authperiod` is 3600 seconds.

The default value of `tx-period` is 30 seconds.

The default value of `supp-timeout` is 30 seconds.

The default value of `server-timeout` is 30 seconds.

Examples

The following is sample output from the `dot1x timeout` command:

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period 4000
```

Related Commands

dot1x reauthentication

show dot1x

7.10 dot1x guest-vlan

Use the `dot1x guest-vlan` interface configuration command to specify an active VLAN as an 802.1x guest VLAN. Use the `no` form of this command to return to the default setting.

Command Syntax

dot1x guest-vlan *vlanid*

no dot1x guest-vlan

<i>vlanid</i>	Specify an active VLAN as an 802.1x guest VLAN. The range is 2 to 4094
---------------	--

Command Mode

Interface Configuration mode

Default

No guest VLAN is configured.

Usage

When you configure a guest VLAN, clients that are not 802.1x-capable are put into the guest VLAN when the server does not receive a response to its Extensible Authentication Protocol over LAN (EAPOL) request/identity frame. Clients that are 802.1x-capable but fail authentication are not granted access to the network.

The guest VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports

Examples

This example shows how to specify VLAN 5 as an 802.1x guest VLAN:

```
Switch(config)#vlan database
Switch(config-vlan)#vlan 5
Switch(config-vlan)#exit
Switch(config)# interface eth-0-1
Switch(config-if)#switchport mode access
Switch(config-if)#dot1x port-control auto
Switch(config-if)#dot1x guest-vlan 5
```

Related Commands

show dot1x

7.11 radius-server deadtime

To improve RADIUS response times when some servers might be unavailable and cause the unavailable servers to be skipped immediately, use the radius-server deadtime command in global configuration mode. To set dead-time to default value, use the no form of this command.

Command Syntax

radius-server deadtime *minutes*

no radius-server deadtime

<i>minutes</i>	Length of time, in minutes, for which a RADIUS server is skipped over by transaction requests, the range is 1 to 20
----------------	---

Default

5 minutes

Command Mode

Global Configuration

Usage

Use this command to cause the switch to mark as “dead” any RADIUS servers that fail to respond to authentication requests, thus avoiding the wait for the request to time out before trying the next configured server. A RADIUS server marked as “dead” is skipped by additional requests for the duration of minutes, unless there are no servers not marked “dead”.

The default value of the radius deadtime is 5 minutes.

Examples

The following is sample output from the radius deadtime command:

```
Switch(config)# radius deadtime 10
```

Related Commands

radius-server host

7.12 radius-server host

To specify a RADIUS server host, use the radius-server host command in global configuration mode. To delete the specified RADIUS host, use the no form of this command.

Command Syntax

radius-server host (**mgmt-if** |)(*ipv4-address* | *ipv6-address*) (**auth-port** *port-number* |) (**timeout** *seconds* |) (**retransmit** *retries* |) (**key** *string*|)

no radius-server host (*ipv4-address* | *ipv6-address*) (**auth-port** *port-number*|)

mgmt-if	Management port
<i>ipv4-address</i>	IPv4 address of the RADIUS server host
<i>ipv6-address</i>	IPv6 address of the RADIUS server host
auth-port <i>port-number</i>	(Optional) Port number for authentication requests; the host is not used for authentication if set to 0. If unspecified, the port number defaults to 1812
timeout <i>seconds</i>	(Optional) Specifies the timeout value. Enter a value in the range 1 to 1000. If no timeout value is specified, the global value is used. The default value should be 5
retransmit <i>retries</i>	(Optional) Specifies the retransmit value. Enter a value in the range 1 to 100. If no retransmit value is specified, the global value is used. The default value should be 3
key <i>string</i>	(Optional) Specifies the authentication and encryption key for all RADIUS communications between the switch and the RADIUS server. This key must match the encryption used on the RADIUS daemon

Command Mode

Global Configuration

Default

None

Usage

You can use multiple radius-server host commands to specify multiple hosts. The software searches for hosts in the order in which you specify them.

If no host-specific timeout, retransmit, or key values are specified, the global values apply to each host.

Examples

The following is sample output from the radius-server host command:

```
Switch(config)# radius-server host 10.10.1.1 key abcde
```

Related Commands

radius-server key

radius-server timeout

7.13 radius-server retransmit

To specify the number of times the switch searches the list of RADIUS server hosts before giving up, use the `radius-server retransmit` command in global configuration mode. To disable retransmission, use the `no` form of this command.

Command Syntax

radius-server retransmit *retries*

no radius-server retransmit

<i>retries</i>	Maximum number of retransmission attempts. The range is 1 to 100. The default is 3
----------------	--

Default

3 attempts

Command Mode

Global Configuration

Usage

The switch tries all servers, allowing each one to time out before increasing the retransmit count.

If the RADIUS server is only a few hops from the switch, we recommend that you configure the RADIUS server retransmit rate to 5.

The default value of radius retransmit is 3 attempts.

Examples

The following is sample output from the radius retransmit command:

```
Switch(config)# radius retransmit 5
```

Related Commands

radius-server host

radius-server key

7.14 radius-server timeout

To set the interval for which a switch waits for a server host to reply, use the `radius-server timeout` command in global configuration mode. To restore the default, use the `no` form of this command.

Command Syntax

radius-server timeout *seconds*

no radius-server timeout

<i>seconds</i>	Number that specifies the timeout interval, in seconds. The range is 1 to 1000. The default is 5 seconds.
----------------	---

Command Mode

Global Configuration

Default

None

Usage

Use this command to set the number of seconds a switch waits for a server host to reply before timing out.

If the RADIUS server is only a few hops from the switch, we recommend that you configure the RADIUS server timeout to 15 seconds.

The default value of radius timeout is 5 seconds.

Examples

The following is sample output from the radius timeout command:

```
Switch(config)# radius retransmit 15
```

Related Commands

radius-server host

radius-server key

7.15 radius-server key

To set the shared encryption key of RADIUS server, use the radius-server key command in global configuration mode. To restore the default, use the no form of this command.

Command Syntax

radius-server key *key-string*

no radius-server key

<i>key-string</i>	RADIUS server key-string
-------------------	--------------------------

Command Mode

Global Configuration

Default

None

Usage

Use this command to set the shared encryption key in a switch.

Shared encryption key is the foundation of communicate between switch and server. You need set a same shared encryption string in authentication server and switch.

Examples

The following is sample output from the radius-server key command:

```
Switch(config)# radius-server key simple-key
```

Related Commands

radius-server host

7.16 show dot1x

Use the show dot1x user EXEC command to display IEEE 802.1x statistics, administrative status, and operational status for the switch or for the specified port.

Command Syntax

show dot1x ((agnostics | session-statistics | statistics) (all | interface *INTERFACE-ID*) | all |)

diagnostics	Display diagnostics of IEEE 802.1x status
session-statistics	Display session statistics of IEEE 802.1x clients
statistics	Display statistics of EAPOL packets
all	Display IEEE 802.1x information of all interfaces
interface <i>INTERFACE-ID</i>	Specify an interface

Command Mode

Privileged EXEC

Default

None

Usage

N/A

Examples

The following is sample output from the show dot1x command:

```
Switch# show dot1x statistics interface eth-0-1
802.1X statistics for interface eth-0-1
  EAPOL Frames Rx: 0 - EAPOL Frames Tx: 323
  EAPOL Start Frames Rx: 0 - EAPOL Logoff Frames Rx: 0
  EAP Rsp/Id Frames Rx: 0 - EAP Response Frames Rx: 0
  EAP Req/Id Frames Tx: 241 - EAP Request Frames Tx: 0
  Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
  EAPOL Last Frame Version Rx: 0 - EAPOL Last Frame Src: 0000.0000.0000
```

Related Commands

dot1x system-auth-ctrl

dot1x port-control

7.17 debug dot1x

Use this command to turn on the debug switches of dot1x module.

To restore the default, use the **no** form of this command

Command Syntax

debug dot1x (event | timer | packet | all)

no debug dot1x (event | timer | packet | all)

event	put out the debug message of dot1x events
timer	put out the debug message of dot1x timer information
packet	put out the debug message of dot1x packets information, include sent and received
all	put out all debug message mentioned above

Command Mode

Privileged EXEC

Default

None

Usage

Use command “**terminal monitor**” to make debug messages print on the VTY immediately.

Use command “**show logging buffer**” to check the debug messages in the logging buffer.

Examples

The following is sample to open dot1x debug switches:

```
Switch# debug dot1x all
```

Related Commands

terminal monitor

show logging buffer

7.18 clear dot1x

Use the clear dot1x user EXEC command to clear the IEEE 802.1x statistics for the switch or for the specified port.

Command Syntax

clear dot1x (statistics | session-statistics) (all |)

statistics	Display statistics of EAPOL packets
session-statistics	Display session statistics of IEEE 802.1x clients
all	Display IEEE 802.1x information of all interfaces

Command Mode

Privileged EXEC

Default

None

Usage

Use the command “**clear dot1x**” to clear the IEEE 802.1x statistics for the switch or for the specified port.

Use the command “**show dot1x**” to display the IEEE 802.1x statistics.

Examples

The following is sample to using the clear dot1x command:

```
Switch# clear dot1x statistics
```

```
Switch# clear dot1x session-statistics
```

Related Commands

dot1x system-auth-ctrl

dot1x port-control

show dot1x

7.19 show radius-server

Use the “show radius-server” command to display radius server states of each IEEE 802.1x session.

Command Syntax

show radius-server

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to display the current radius-server and dead radius-servers of each IEEE 802.1 x sessions.

Examples

The following is sample output from the show radius-server command:

```
Switch# show radius-server
=====
802.1X session on interface eth-0-9:
current radius server:
  retransmit count : 3
  server address   : 3.3.3.3:1812
  socket descriptor : 15
  last state      :
radius servers in dead list:
N/A
=====
```

```
Switch # show radius-server
=====
802.1X session on interface eth-0-9:
current radius server:
N/A
radius servers in dead list:
server address   : 3.3.3.3:1812
socket descriptor : 15
last state      :
=====
```

Related Commands

radius-server host

7.20 dot1x re-active radius-server

Use the “dot1x re-active” command to active the specified radius servers.

Command Syntax

dot1x re-active radius-server (host *A.B.C.D* (auth-port *PORT*)| interface *IFPHYSICAL* | all)

host <i>A.B.C.D</i> (auth-port <i>PORT</i>)	Re-active the radius-server by server ip and udp port
interface <i>IFPHYSICAL</i>	Re-active the radius-servers by IEEE 802.1x client’s interface
all	Re-active all radius-servers

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to active the radius server. Users do not need the wait for the radius-server dead time with this command.

Examples

The following is samples to use the dot1x re-active radius-server command::

```
Switch # dot1x re-activate radius-server
Switch # dot1x re-activate radius-server host 3.3.3.3 auth-port 1812
Switch # dot1x re-activate radius-server interface eth-0-9
```

Related Commands

radius-server host

radius-server deadtime

show radius-server

8

Arp Inspection Commands

8.1 show ip arp inspection

Use this command to display the configuration of arp inspection.

Command Syntax

show ip arp inspection

Command Mode

Privileged EXEC

Default

No default is defined.

Usage

This command is used to show the general configuration of arp inspection.

Examples

This example shows how to display the information of arp inspection.

```
Switch # show ip arp inspection
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

Vlan    Configuration    ACL Match    Static ACL
=====
1       enabled         acl
=====

Vlan    ACL Logging    DHCP Logging
=====
1       deny          deny
=====

Vlan    Forwarded    Dropped    DHCP Drops    ACL Drops
=====
1       0            0          0             0
=====

Vlan    DHCP Permits    ACL Permits    Source MAC Failures
=====
1       0            0            0
=====

Vlan    Dest MAC Failures    IP Validation Failures    Invalid Protocol Data
=====
1       0                    0                          0
=====
```

Related Commands

ip arp inspection vlan

8.2 show ip arp inspection interfaces

Use this command to display the arp inspection configuration of specified interface.

Command Syntax

show ip arp inspection interfaces (*IFNAME*)

IFNAME	Interface name
--------	----------------

Command Mode

Privileged EXEC

Default

No default is defined.

Usage

This command is used to show the arp inspection configuration on interface.

Examples

This example shows how to display all the arp inspection configuration of all interface.

```
Switch# show ip arp inspection interfaces
Interface      Trust State
=====
eth-0-1        untrusted
eth-0-2        untrusted
eth-0-3        untrusted
eth-0-4        untrusted
eth-0-5        untrusted
eth-0-6        untrusted
eth-0-7        untrusted
eth-0-8        untrusted
eth-0-9        untrusted
eth-0-10       untrusted
eth-0-11       untrusted
eth-0-12       untrusted
eth-0-13       untrusted
eth-0-14       untrusted
eth-0-15       untrusted
eth-0-16       untrusted
eth-0-17       untrusted
eth-0-18       untrusted
eth-0-19       untrusted
eth-0-20       untrusted
eth-0-21       untrusted
eth-0-22       untrusted
eth-0-23       untrusted
eth-0-24       untrusted
```

```
eth-0-25      untrusted
eth-0-26      untrusted
eth-0-27      untrusted
eth-0-28      untrusted
eth-0-29      untrusted
eth-0-30      untrusted
eth-0-31      untrusted
eth-0-32      untrusted
eth-0-33      untrusted
eth-0-34      untrusted
eth-0-35      untrusted
eth-0-36      untrusted
eth-0-37      untrusted
eth-0-38      untrusted
eth-0-39      untrusted
eth-0-40      untrusted
eth-0-41      untrusted
eth-0-42      untrusted
eth-0-43      untrusted
eth-0-44      untrusted
eth-0-45      untrusted
eth-0-46      untrusted
eth-0-47      untrusted
eth-0-48      untrusted
```

Related Commands

ip arp inspection trust

8.3 show ip arp inspection log

Use this command to display the log configuration and log information in arp inspection log buffer. The default number is 32.

Command Syntax

show ip arp inspection log (*number*)

number	Specify the number of message, range is 1 to 1024
--------	---

Command Mode

Privileged EXEC

Default

No default is defined.

Usage

This command is used to verify arp inspection log settings.

Examples

This example shows how to display the log information in arp inspection log buffer.

```
Switch # show ip arp inspection log
Total Log Buffer Size : 32
```

```
Syslog rate : 5 entries per 1 seconds.
No entries in log buffer
```

Related Commands

ip arp inspection log-buffer

8.4 show ip arp inspection statistics

Use this command to displays statistics for forwarded, dropped, MAC validation failure, IP validation failure, ACL permitted and denied, and DHCP permitted and denied packets for the specified vlan. If no vlans are specified or if a range is specified, displays information only for vlans with ARP Inspection enabled.

Command Syntax

show ip arp inspection statistics (vlan *vlan_id*)

vlan <i>vlan_id</i>	Selected vlan range
----------------------------	---------------------

Command Mode

Privileged EXEC

Default

No default is defined.

Usage

Displays statistics for forwarded, dropped, MAC validation failure, IP validation failure, ACL permitted and denied, and DHCP permitted and denied packets for the specified VLAN.

Examples

This example shows how to display the arp inspection statistics.

```
Switch # show ip arp inspection statistics vlan 1

Vlan    Forwarded    Dropped    DHCP Drops    ACL Drops
=====
1       0             0           0             0

Vlan    DHCP Permits  ACL Permits  Source MAC Failures
=====
1       0             0           0

Vlan    Dest MAC Failures  IP Validation Failures  Invalid Protocol Data
=====
1       0                   0                       0
```

Related Commands

clear ip arp inspection statistics

8.5 show ip arp inspection vlan

Use this command to displays the configuration and the operating state of ARP Inspection for the specified vlan.

Command Syntax

show ip arp inspection vlan *vlan_id*

vlan <i>vlan_id</i>	Selected vlan range
----------------------------	---------------------

Command Mode

Privileged EXEC

Default

No default is defined.

Usage

If no vlans are specified or if a range is specified, displays information only for vlans with ARP Inspection enabled.

Examples

This example shows how to display the arp inspection statistics

```
Switch # show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan  Configuration      ACL Match  Static ACL
=====
1      enabled           acl
Vlan  ACL Logging      DHCP Logging
=====
1      deny             deny
```

Related Commands

ip arp inspection vlan

8.6 show debugging arp inspection

Use this command to display the debug information of ARP Inspection.

Command Syntax

show debugging arp inspection

Command Mode

Privileged EXEC

Default

No default is defined.

Usage

This command is used to show the general configuration of arp inspection.

Examples

This example shows how to display the debug information of ARP Inspection.

```
Switch # show debugging arp inspection
arp inspection debugging status:
  packet debugging is on
  error debugging is on
```

Related Commands

`debug arp inspection`

8.7 debug arp inspection

Use this command to configure ARP Inspection debug.

Command Syntax

debug arp inspection (all|packet|events|error)

all	Turn all debugging on
packet	ARP message fields
events	ARP Inspection events
error	Error DHCP message

Command Mode

Privileged EXEC

Default

All debug disabled.

Usage

This command is used to debug arp inspection, including all, error, events, packet.

Examples

This example shows how to use this command to debug all error ARP packet.

```
Switch # debug ip arp inspection error
```

Related Commands

show debugging arp inspection

8.8 ip arp inspection filter vlan

Use this command to applies the ARP ACL to a VLAN.

Command Syntax

ip arp inspection filter *acl* vlan *vlan_id* (static)

acl	ARP acl name
vlan_id	Selected vlan range
static	Apply the ACL statically

Command Mode

Global Configuration

Default

No default is defined.

Usage

This command is used to show the general configuration of arp inspection.

Examples

This example shows how to apply the ARP ACL to a vlan 2.

```
Switch(config)# ip arp inspection filter acl vlan 2 static
```

Related Commands

arp access-list

8.9 ip arp inspection log-buffer entries

Use this command to set log-buffer size.

Command Syntax

ip arp inspection log-buffer entries *number*

number	Number of log buffer, range is 10 to 1024
--------	---

Command Mode

Privileged EXEC

Default

None

Usage

The no command reverts the log-buffer to the default buffer size (32).

Examples

This example shows how to set log-buffer size to 10.

```
Switch(config)# ip arp inspection log-buffer entries 10
```

Related Commands

show ip arp inspection log

8.10 [no] ip arp inspection log-buffer logs interval

Use this command to configure the DAI logging system messages. The no command reverts the default system message configuration.

Command Syntax

ip arp inspection log-buffer logs *number interval interval*

number	Number of log buffer, range is 10 to 1024
interval	Interval (seconds), range is 0 to 86400

Command Mode

Global Configuration

Default

No default is defined.

Usage

A 0 value for the logs number indicates that the entries should not be logged out of this buffer. The default number is 5.

A 0 value for the interval seconds keyword and argument indicates an immediate log. The default number is 1.

Examples

This example shows how to configure logging to send 12 messages every 2 seconds.

```
Switch(config)# ip arp inspection log-buffer logs 12 interval 2
```

8.11 ip arp inspection validate

Use this command to enable additional validation on the destination MAC address, the sender and target IP addresses, and the source MAC address.

Command Syntax

[no] ip arp inspection validate (dst-mac|ip|src-mac)

dst-mac	Validate destination MAC address
ip	Validate IP addresses
src-mac	Validate source MAC address

Command Mode

Global Configuration

Default

No default is defined.

Usage

For `src-mac`, check the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

For `dst-mac`, check the destination MAC address in the Ethernet header against the target MAC address in ARP body. This check is performed for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.

For `ip`, check the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses.

Examples

This example shows how to enable additional validation on the destination MAC address.

```
Switch(config)# ip arp inspection validate dst-mac
```

Related Commands

show ip arp inspection

8.12 ip arp inspection vlan

Use this command to enable ARP Inspection on vlans.

Command Syntax

[no] ip arp inspection vlan *vlan_id*

vlan_id	Vlan range, example: 1,3-5,7,9-11
---------	-----------------------------------

Command Mode

Global Configuration

Default

No default is defined.

Usage

Enable ARP Inspection on vlans.

Examples

This example shows how to enable ARP Inspection on VLAN 2.

```
Switch(config)# ip arp inspection vlan 2
```

Related Commands

show ip arp inspection vlan 2

8.13 ip arp inspection vlan logging acl-macth

Use this command to configure ARP Inspection log filtering.

Command Syntax

[no] ip arp inspection vlan *vlan_id* logging acl-macth (matchlog|none)

vlan_id	Vlan range, example: 1,3-5,7,9-11
matchlog	Log packets on ACE logging configuration
none	Do not log packets that match ACLs

Command Mode

Global Configuration

Default

No default is defined.

Usage

If you specify the matchlog keyword in this command and the log keyword in the permit or deny ARP access-list configuration command, ARP packets permitted or denied by the ARP Inspection are logged.

Examples

This example shows how to log permitted ARP packets on vlan 2.

```
Switch(config)# ip arp inspection vlan 2 logging acl-match matchlog
```

Related Commands

ip arp inspection vlan

8.14 ip arp inspection vlan logging dhcp-bindings

Use this command to configure ARP Inspection log filtering.

Command Syntax

[no] ip arp inspection vlan *vlan_id* logging dhcp-bindings (all|none|permit)

vlan_id	Vlan range, example: 1,3-5,7,9-11
all	Log all packets that match DHCP bindings
permit	Log DHCP Binding Permitted packets
none	Do not log packets that match DHCP bindings

Command Mode

Global Configuration

Default

No default is defined.

Usage

If the command is set, the information that match the dhcp-bings will be logged.

Examples

This example shows how to Logs all packets that match DHCP bindings on vlan 2.

```
Switch(config)# ip arp inspection vlan 2 logging dhcp-bindings all
```

Related Commands

show ip arp inspection vlan

8.15 clear ip arp inspection log-buffer

Use this command to delete all log in log-buffer.

Command Syntax

clear ip arp inspection log-buffer

Command Mode

Privileged EXEC Default

No default is defined.

Usage

This command is used to delete all log in log-buffer.

Examples

This example shows how to delete all log in log-buffer.

```
Switch# clear ip arp inspection log-buffer
```

Related Commands

ip arp inspection log-buffer logs

8.16 clear ip arp inspection statistics

Use this command to delete all statistics of ARP Inspection.

Command Syntax

clear ip arp inspection statistics

Command Mode

Global Configuration

Default

No default is defined.

Usage

This command is used to delete all statistics of ARP Inspection.

Examples

This example shows how to delete all statistics of ARP Inspection.

```
Switch(config)# clear ip arp inspection statistics
```

Related Commands

show ip arp inspection statistics

8.17 ip arp inspection trust

Use this command to configure the ARP Inspection interface trust state.

Command Syntax

ip arp inspection trust
no ip arp inspection trust

Command Mode

Interface configuration

Default

No default is defined.

Usage

In a typical network configuration, you configure all switch ports connected to host ports as untrusted and configure all switch ports connected to switches as trusted.

Examples

This example shows how to configure the ARP Inspection interface eth-0-2 untrusted state.

```
Switch(config-if)# no ip arp inspection trust
```

Related Commands

show ip arp inspection interfaces

8.18 arp access-list

Use this command to configure a ARP ACL

Command Syntax

arp access-list *acl*
no arp access-list *acl*

acl	A arp access-list name
-----	------------------------

Command Mode

Global Configuration

Default

No default is defined.

Usage

In non-DHCP environments, dynamic ARP inspection can validate ARP packets against user-configured ARP access control lists (ACLs) for hosts with statically configured IP addresses.

Examples

This example shows how to configure a ARP ACL.

```
Switch(config)# arp access-list acl1
```

Related Commands

show access-list arp

8.19 ip mac

Use this command to configure ARP ACEs.

Command Syntax

(deny|permit) (request | response |) ip (address wildcard|any|host address) mac (MAC MASK|any|host MAC) (log |)

deny	Specify packets to reject
permit	Log all packets that match DHCP bindings
request	Log DHCP Binding Permitted packets
response	Do not log packets that match DHCP bindings
address	Sender address
wildcard	Sender wildcard bits
any	Any sender host
host	A single Sender host
MAC	Sender host's MAC address in HHHH.HHHH.HHHH format
MASK	Sender wildcard in HHHH.HHHH.HHHH format
log	Log at match

Command Mode

ARP-ACL

Default

No default is defined.

Usage

Use this command to add ARP ACE to ARP ACL.

Examples

This example shows how to configure a ARP ACE.

```
Switch(config-arp-acl)# permit ip host 192.168.1.1 mac any
```

Related Commands

show access-list arp

8.20 no sequence-num

Use this command to delete a ARP ACE.

Command Syntax

no sequence-num *number*

number	Specify a sequence number, range is 1 to 2147483646
--------	---

Command Mode

ARP-ACL

Default

No default is defined.

Usage

This command is used to delete ARP ACE configured.

Examples

This example shows how to delete a ARP ACE

```
Switch(config-arp-acl)# no sequence-num 10
```

Related Commands

show access-list arp

8.21 show access-list arp

Use this command to display the arp acl configuration.

Command Syntax

show access-list arp (*acl*)

acl	A arp access-list name
-----	------------------------

Command Mode

Privileged EXEC

Default

No default is defined.

Usage

This command is used to display the arp acl configured by arp acl.

Examples

This example shows how to display arp ace.

```
Switch # show access-list arp
arp access-list acl
10 permit request ip 1.1.1.1 0.255.255.255 mac any
```


Related Commands

`arp access-list`

9 DHCP Snooping Commands

9.1 clear dhcp snooping

Use the clear dhcp snooping global configuration command on the switch to clear dynamic entries in DHCP binding database or the DHCP snooping statistics counters.

Command Syntax

clear dhcp snooping (bindings learning (ipv4 *IP-ADDRESS* | mac *MAC-ADDRESS* | vlan *VLAN-ID* | interface *IFNAME*) | statistics)

bindings	Clear the DHCP snooping binding database
ipv4 <i>IP-ADDRESS</i>	Clear the binding entry by IP address
mac <i>MAC-ADDRESS</i>	Clear the binding entry by MAC address
vlan <i>VLAN-ID</i>	Clear the binding entry by VLAN
interface <i>IFNAME</i>	Clear the binding entry by interface
statistics	Clear the DHCP snooping statistics counter

Command Mode

Global Configuration

Default

No default is defined.

Usage

This command is used to clear DHCP snooping binding or statistics.

Examples

This example shows how to clear the DHCP snooping statistics counters:

```
Switch(config)# clear dhcp snooping statistics
```

Related Commands

show dhcp snooping binding

show dhcp snooping statistics

9.2 dhcp snooping

Use the dhcp snooping global configuration command on the switch to globally enable DHCP snooping. Use the no form of this command to return to the default setting.

Command Syntax

dhcp snooping

no dhcp snooping

Command Mode

Global Configuration

Default

DHCP snooping is disabled.

Usage

For any DHCP snooping configuration to take effect, you must globally enable DHCP snooping. DHCP snooping is not active until you enable snooping on a VLAN by using the `dhcp snooping vlan vlan-id` global configuration command.

Examples

This example shows how to enable DHCP snooping:

```
Switch(config)# dhcp snooping
```

You can verify your settings by entering the `show dhcp snooping config` privileged EXEC command.

Related Commands

dhcp snooping vlan

show dhcp snooping config

9.3 dhcp snooping binding

Use the `dhcp snooping binding` global configuration command on the switch to configure the DHCP snooping binding database and to add binding entries to the database.

Command Syntax

dhcp snooping binding mac *MAC-ADDRESS* **vlan** *VLAN-ID* **ipv4** *IP-ADDRESS* **interface** *IFNAME* **expiry** *SECONDS*

no dhcp snooping bindings (**ipv4** *IP-ADDRESS* | **mac** *MAC-ADDRESS* | **vlan** *VLAN-ID* | **interface** *IFNAME* |)

mac <i>MAC-ADDRESS</i>	Specify a MAC address
vlan <i>VLAN-ID</i>	Specify a VLAN number. The range is 1 to 4094
ipv4 <i>IP-ADDRESS</i>	Specify an IP address
interface <i>IFNAME</i>	Specify an interface on which to add or delete a binding entry
expiry <i>SECONDS</i>	Specify the interval (in seconds) after which the binding entry is no longer valid. The range is 0 to 86400

Command Mode

Global Configuration

Default

No default database is defined.

Usage

Use this command when you are testing or debugging the switch.

In the DHCP snooping binding database, each database entry, also referred to a binding, has an IP address, an associated MAC address, the lease time, the interface to which the binding applies, and the VLAN to which the interface belongs.

Use the `show dhcp snooping binding` privileged EXEC command to display the configured bindings.

Examples

This example shows how to generate a DHCP binding configuration with an expiration time of 1000 seconds on a port in VLAN 1:

```
Switch(config)# dhcp snooping binding mac 0001.000c.01ef vlan 1 ipv4 10.10.1.1 interface eth-0-1 expiry 1000
```

Related Commands

dhcp snooping

show dhcp snooping binding

9.4 dhcp snooping database

Use the `dhcp snooping database global configuration` command on the switch to configure the DHCP snooping binding database agent. Use the `no` form of this command to disable the agent, to reset the timeout value, or to reset the write-delay value.

Command Syntax

dhcp snooping database auto-save interval *SECONDS*

interval <i>SECONDS</i>	Specify the interval (in seconds) that how long to save the binding database. The range is 15 to 1200
--------------------------------	---

Command Mode

Global Configuration

Default

Default interval is 600 seconds.

Usage

The DHCP snooping database is save as `flash:/dhcpsnooping`.

Examples

The following is sample output from the `dhcp snooping database` command:

```
Switch(config)# dhcp snooping database auto-save interval 120
```

Related Commands

dhcp snooping

dhcp snooping binding

9.5 dhcp snooping information option

Use the `dhcp snooping information option` global configuration command on the switch to enable DHCP option-82 data insertion. Use the `no` form of this command to disable DHCP option-82 data insertion.

Command Syntax

dhcp snooping information option

no dhcp snooping information option

Command Mode

Global Configuration

Default

DHCP option-82 data is not inserted.

Usage

You must globally enable DHCP snooping by using the `dhcp snooping global configuration` command for any DHCP snooping configuration to take effect.

When the option-82 feature is enabled and a switch receives a DHCP request from a host, it adds the option-82 information in the packet. The option-82 information contains the switch MAC address (the remote ID suboption) and the port identifier, `vlan-mod-port`, from which the packet is received (circuit ID suboption). The switch forwards the DHCP request that includes the option-82 field to the DHCP server.

When the DHCP server receives the packet, it can use the remote ID, the circuit ID, or both to assign IP addresses and implement policies, such as restricting the number of IP addresses that can be assigned to a single remote ID or a circuit ID. Then the DHCP server echoes the option-82 field in the DHCP reply.

The DHCP server unicasts send the reply to the switch if the request has been relayed to the server by the switch. When the client and server are on the same subnet, the server broadcasts the reply. The switch inspects the remote ID and possibly the circuit ID fields to verify that it originally inserted the option-82 data. The switch removes the option-82 field and forwards the packet to the switch port that connects to the DHCP host that sent the DHCP request.

Examples

This example shows how to enable DHCP option-82 data insertion:

```
Switch(config)# dhcp snooping information option
```

You can verify your settings by entering the `show dhcp snooping config` privileged EXEC command.

Related Commands

show dhcp snooping config

show dhcp snooping binding

9.6 dhcp snooping information option allow-untrusted

Use the dhcp snooping information option allow-untrusted global configuration command on an aggregation switch to configure it to accept DHCP packets with option-82 information that are received on untrusted ports that might be connected to an edge switch. Use the no form of this command to return to the default setting.

Command Syntax

dhcp snooping information option allow-untrusted
no dhcp snooping information option allow-untrusted

Command Mode

Global Configuration

Default

The switch drops DHCP packets with option-82 information that are received on untrusted ports that might be connected to an edge switch.

Usage

You might want an edge switch to which a host is connected to insert DHCP option-82 information at the edge of your network. You might also want to enable DHCP security features, such as DHCP snooping, IP source guard, or dynamic Address Resolution Protocol (ARP) inspection, on an aggregation switch. However, if DHCP snooping is enabled on the aggregation switch, the switch drops packets with option-82 information that are received on an untrusted port and does not learn DHCP snooping bindings for connected devices on a trusted interface.

If the edge switch to which a host is connected inserts option-82 information and you want to use DHCP snooping on an aggregation switch, enter the dhcp snooping information option allow-untrusted command on the aggregation switch. The aggregation switch can learn the bindings for a host even though the aggregation switch receives DHCP snooping packets on an untrusted port. You can also enable DHCP security features on the aggregation switch. The port on the edge switch to which the aggregation switch is connected must be configured as a trusted port.

Examples

This example shows how to configure an access switch to not check the option-82 information in untrusted packets from an edge switch and to accept the packets:

```
Switch(config)# dhcp snooping information option allow-untrusted
```

Related Commands

show dhcp snooping config

9.7 dhcp snooping trust

Use the dhcp snooping trust interface configuration command on the switch to configure a port as trusted for DHCP snooping purposes. Use the no form of this command to return to the default setting.

Command Syntax

dhcp snooping trust
no dhcp snooping trust

Command Mode

Interface configuration

Default

DHCP snooping trust is disabled.

Usage

Configure as trusted ports those that are connected to a DHCP server or to other switches or routers. Configure as untrusted ports those that are connected to DHCP clients.

Examples

This example shows how to enable DHCP snooping trust on a port:

```
Switch(config-if)# dhcp snooping trust
```

Related Commands

show dhcp snooping config

9.8 dhcp snooping verify

Use the `dhcp snooping verify` global configuration command on the switch to configure the switch to verify on an untrusted port that the source MAC address in a DHCP packet matches the client hardware address. Use the `no` form of this command to configure the switch to not verify the MAC addresses.

Command Syntax

dhcp snooping verify mac-address

no dhcp snooping verify mac-address

Command Mode

Global Configuration

Default

The switch verifies the source MAC address in a DHCP packet that is received on untrusted ports matches the client hardware address in the packet.

Usage

In a service-provider network, when a switch receives a packet from a DHCP client on an untrusted port, it automatically verifies that the source MAC address and the DHCP client hardware address match. If the addresses match, the switch forwards the packet. If the addresses do not match, the switch drops the packet.

Examples

This example shows how to disable the MAC address verification:

```
Switch(config)# no dhcp snooping verify mac-address
```

Related Commands

show dhcp snooping config

9.9 dhcp snooping vlan

Use the `dhcp snooping vlan` global configuration command on the switch to enable DHCP snooping on a VLAN. Use the `no` form of this command to return to the default setting.

Command Syntax

dhcp snooping vlan *VLAN-RANGE*

no dhcp snooping vlan *VLAN-RANGE*

VLAN-RANGE	Specify a VLAN ID or a range of VLANs on which to enable DHCP snooping. The range is 1 to 4094
------------	--

Command Mode

Global Configuration

Default

DHCP snooping is disabled on all VLANs.

Usage

You can enter a single VLAN ID identified by VLAN ID number, a series of VLAN IDs separated by commas, a range of VLAN IDs separated by hyphens, or a range of VLAN IDs separated by entering the starting and ending VLAN IDs separated by a space.

You must first globally enable DHCP snooping before enabling DHCP snooping on a VLAN.

Examples

This example shows how to enable DHCP snooping on VLAN 10:

```
Switch(config)# dhcp snooping vlan 10
```

Related Commands

show dhcp snooping config

9.10 dhcp snooping vlan information option format-type circuit-id string

Use this interface configuration command on the switch stack or on a standalone switch to configure the option-82 circuit-ID suboption. Use the `no` form of this command to configure the default circuit-ID suboption.

Command Syntax

dhcp snooping vlan *VLAN-ID* **information option format-type circuit-id string** *STRING*

no dhcp snooping vlan *VLAN-ID* **information option format-type circuit-id string**

vlan <i>VLAN-ID</i>	Specify a VLAN ID. The range is 1 to 4094
<i>STRING</i>	Use string for circuit id (1-63 chars)

Command Mode

Interface Configuration

Default

None

Usage

User must globally enable DHCP snooping configuration command for any DHCP snooping configuration to take effect.

Examples

This example shows how configure the option-82 circuit-ID suboption:

```
Switch(config-if) # dhcp snooping vlan 2 information option format-type circuit-id string  
vlan2
```

Related Commands

None

9.11 dhcp snooping information option format remote-id

Use the `dhcp snooping information option format remote-id` global configuration command on the switch stack or on a standalone switch to configure the option-82 remote-ID suboption. Use the `no` form of this command to configure the default remote-ID suboption.

Command Syntax

dhcp snooping information option format remote-id (string *NAME* | hostname)

no dhcp snooping information option format remote-id

string <i>NAME</i>	Specify a remote ID, using from 1 to 63 ASCII characters (no spaces)
hostname	Specify the switch hostname as the remote ID

Command Mode

Global Configuration

Default

None

Usage

You must globally enable DHCP snooping configuration command for any DHCP snooping configuration to take effect.

Examples

This example shows how configure the option-82 remote-ID suboption:

```
Switch(config) # dhcp snooping information option format remote-id hostname
```

Related Commands

None

9.12 debug dhcp snooping

Use this command to turn on the debug switches of dhcp snooping module.

To restore the default, use the **no** form of this command

Command Syntax

debug dhcp snooping (**events** | **error** | **dump** | **packet** | **all**)

no debug dhcp snooping (**events** | **error** | **dump** | **packet** | **all**)

events	Snooping events
error	Error DHCP message
packet	DHCP message fields
dump	Dump message in hex format
all	Turn all debugging on

Command Mode

Privileged EXEC

Default

None

Usage

Use command "**terminal monitor**" to make debug messages print on the VTY immediately.

Use command "**show logging buffer**" to check the debug messages in the logging buffer.

Examples

The following is sample to open dhcp snooping debug switches:

```
Switch# debug dhcp snooping all
```

Related Commands

terminal monitor

show logging buffer

9.13 show dhcp snooping binding

Use the show dhcp snooping binding privileged EXEC command to display the DHCP snooping binding database and configuration information for all interfaces on a switch.

Command Syntax

show dhcp snooping binding ((**all** | **manual** | **learning**) (**ipv4** *IP-ADDRESS* | **mac** *MAC-ADDRESS* | **vlan** *VLAN-ID* | **interface** *IFNAME* |) **summary**)

all	Display all entries
manual	Display static entries
learning	Display dynamic entries
mac <i>MAC-ADDRESS</i>	Specify MAC address
vlan <i>VLAN-ID</i>	Specify a VLAN number. The range is 1 to 4094
ipv4 <i>IP-ADDRESS</i>	Specify an IP address
interface <i>IFNAME</i>	Specify an interface on which to add or delete a binding entry
summary	Display summary information of DHCP snooping bindings

Command Mode

Privileged EXEC

Default

None

Usage

If DHCP snooping is enabled and an interface changes to the down state, the switch does not delete the statically configured bindings.

Examples

The following is sample output from the show dhcp snooping binding command:

```
Switch# show dhcp snooping binding all
DHCP snooping binding table:
VLAN MAC Address   Interface Lease(s)  IP Address
=====
1    0001.0001.0001 eth-0-2   static    1.1.1.1
```

Related Commands

dhcp snooping binding

9.14 show dhcp snooping config

Use the show dhcp snooping privileged EXEC command to display the DHCP snooping configuration.

Command Syntax

show dhcp snooping config

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display the configuration of DHCP snooping.

Examples

The following is sample output from the show dhcp snooping config command:

```
Switch# show dhcp snooping config
dhcp snooping service: enabled
dhcp snooping switch: enabled
Verification of hwaddr field: enabled
Insertion of relay agent information (option 82): enabled
Relay agent information (option 82) on untrusted port: not allowed
dhcp snooping vlan 1
```

Related Commands

dhcp snooping binding

9.15 show dhcp snooping statistics

Use the show dhcp snooping statistics privileged EXEC command to display DHCP snooping statistics.

Command Syntax

show dhcp snooping statistics

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display the statistics of DHCP snooping.

Examples

The following is sample output from the show dhcp snooping statistics command:

```
Switch# show dhcp snooping statistics

DHCP snooping statistics:
=====
DHCP packets                11257
BOOTP packets                0

Packets forwarded           10381
Packets invalid              844
Packets MAC address verify failed 354
Packets dropped              516
```

Related Commands

clear dhcp snooping statistics

9.16 show dhcp snooping trusted-sources

Use the show dhcp snooping trusted-sources command to display DHCP snooping trusted interfaces.

Command Syntax

show dhcp snooping trusted-sources

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to display the trusted interfaces of DHCP snooping.

Examples

The following is sample output from the show dhcp snooping trusted-sources command:

Switch# show dhcp snooping trusted-sources

```
List of DHCP snooping trusted interface(s):
```

```
=====
eth-0-2
```

Related Commands

dhcp snooping trust

10 IP Source Guard Commands

10.1 ip source binding

Use the ip source binding global configuration command on the switch to configure static IP source bindings on the switch. Use the no form of this command to delete static bindings.

Command Syntax

ip source binding mac *MAC-ADDRESS* **vlan** *VLAN-ID* **ip** *IP-ADDRESS* **interface** *INTERFACE-ID*

no ip source binding mac *MAC-ADDRESS* **vlan** *VLAN-ID* **ip** *IP-ADDRESS* **interface** *INTERFACE-ID*

<i>MAC-ADDRESS</i>	Specify a MAC address
<i>VLAN-ID</i>	Specify a VLAN number. < 1 to 4094 >
<i>IP-ADDRESS</i>	Specify an IP address
<i>INTERFACE-ID</i>	Specify an interface on which to add or delete a binding entry

Command Mode

Global Configuration

Default

None

Usage

A static IP source binding entry has an IP address, its associated MAC address, and its associated VLAN number.

The same MAC and IP can only be bound in one binding entry. Duplication of MAC or IP in binding entries is not allowed.

No IP source bindings are configured by default.

Examples

The following is sample output from the ip source binding command:

```
Switch(config)# ip source binding mac 0001.1234.1234 vlan 1 ip 172.20.50.5 interface eth-0-1
```

Related Commands

show ip source binding

no ip source binding

10.2 no ip source binding

Use the clear ip source binding global configuration command on the switch to no static IP source bindings on the switch.

Command Syntax

no ip source binding entries

no ip source binding entries vlan *VLAN-ID*

no ip source binding entries interface *INTERFACE-ID*

<i>VLAN-ID</i>	Specify a VLAN number. < 1 to 4094 >
<i>INTERFACE-ID</i>	Specify an interface on which to add or delete a binding entry

Command Mode

Global Configuration

Default

None

Usage

If neither vlan-id nor interface-id is specified, all static ip source binding entries will be deleted.

Examples

The following is sample output from the clear ip source binding command:

```
Switch(config)# no ip source binding entries interface eth-0-1
Switch(config)# no ip source binding entries vlan 2
Switch(config)# no ip source binding entries
```

Related Commands

ip source binding

show ip source binding

10.3 ip source maximal binding

To specify the maximum number of bindings for each interface, use the ip source maximal binding command in global configuration mode. To restore to the default value, use the no form of this command.

Command Syntax

ip source maximal binding number per-port *NUMBER*

no ip source maximal binding number per-port

<i>NUMBER</i>	Specify maximum number of bindings. The range is 0 to 30
---------------	--

Command Mode

Global Configuration

Default

None

Usage

Using for configuring maximal binding number, and default value is 10.

Examples

The following example shows how to specify the maximum number of bindings:

```
Switch(config)# ip source maximal binding number per-port 20
```

Related Commands

show ip source binding

10.4 ip verify source

Use the **ip verify source** interface configuration command on the switch stack or on a standalone switch to enable IP source guard on an interface. Use the no form of this command to disable IP source guard.

Command Syntax

ip verify source (ip | ip-mac | ip-vlan | ip-mac-vlan)

no ip verify source

ip	Check only IP address
ip-mac	Check IP address and MAC address
ip-vlan	Check IP address and VLAN
ip-mac-vlan	Check IP address, MAC address, and VLAN

Command Mode

Interface Configuration

Default

None

Usage

When IP source guard is enabled on an access port, the ip-mac-vlan keyword is equivalent to the ip-mac keyword.

By default, IP source guard is disabled on interfaces.

Examples

The following example shows how to enable IP source guard on an interface:

```
Switch(config-if)# ip verify source ip-mac
```

Related Commands

ip source binding

show ip source binding

10.5 show ip source binding

Use the show ip source binding privileged EXEC command to display the IP source bindings on the switch.

Command Syntax

show ip source binding (interface *INTERFACE-ID*)

interface <i>INTERFACE-ID</i>	Display IP source bindings for a specified interface
--------------------------------------	--

Command Mode

Privileged EXEC

Default

None

Usage

If interface is not specified, all ip-source-binding entries should be shown.

Examples

The following is sample output from the show ip source binding command:

```
Switch# show ip source binding
The total number of ip binding is 1, the max ip number limit is 127
The total number of ipv6 binding is 0, the max ipv6 number limit is 128
IP source guard binding table:
VLAN MAC Address   Type   Interface   State   IP Address
=====
3    0001.0002.0003  static eth-0-1    ip      10.0.0.2
```

Related Commands

ip source binding

no ip source binding

11 RADIUS Authentication Commands

11.1 aaa new-model

Enable the authentication, authorization, accounting (AAA) access control model.

Command Syntax

aaa new-model
no aaa new-model

Command Mode

Global Configuration

Default

None

Usage

Enables the AAA access control model

Examples

The following example shows how to enable AAA access control model:

```
Switch# configure terminal
Switch(config)# aaa new-model
```

Related Commands

show aaa status

11.2 aaa authentication login

Set authentication, authorization, accounting (AAA) authentication at login.

Command Syntax

aaa authentication login (default|*LISTNAME*)
{enable|line|none|radius|local|tacacs-plus}
no aaa authentication login (default|*LISTNAME*)

default	Default method list
<i>LISTNAME</i>	An authentication list with this name
enable	Enable password
line	Line password
none	No authentication
radius	RADIUS server

local	Local username
tacacs-plus	TACACS+

Command Mode

Global Configuration

Default

None

Usage

Use the aaa authentication login global configuration command to specify one or more AAA methods for use on ports running IEEE 802.1x.

Examples

The following example shows how to set authentication at login:

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authentication login default local radius none
```

Related Commands

show aaa method-lists authentication

11.3 aaa authorization exec

Set authentication, authorization, accounting (AAA) authorization at login.

Command Syntax

aaa authorization exec (default|LISTNAME) { none|radius|local|tacacs-plus}

no aaa authorization exec (default|LISTNAME)

default	Default method list
<i>LISTNAME</i>	An authentication list with this name
none	No authentication
radius	RADIUS server
local	Local username
tacacs-plus	TACACS+

Command Mode

Global Configuration

Default

None

Usage

Use the aaa authorization exec global configuration command to specify one or more AAA authorization methods for use on ports running IEEE 802.1x.

Examples

The following example shows how to set authorization at login:

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa authorization exec default local radius none
```

Related Commands

11.4 aaa accounting exec

Set authentication, authorization, accounting (AAA) accounting at login.

Command Syntax

aaa accounting exec (default|*LISTNAME*) (((start-stop|stop-only) {radius|tacacs-plus} (none|)) | none)

no aaa accounting exec (default|*LISTNAME*)

default	Default method list
<i>LISTNAME</i>	An accounting list with this name
start-stop	Send exec accounting start and stop request while logging switch
stop-only	Only send exec accounting stop request while exit switch
none	No accounting
radius	RADIUS server
tacacs-plus	TACACS+

Command Mode

Global Configuration

Default

None

Usage

Use the aaa accounting exec global configuration command to specify one or more AAA accounting methods for use on ports running IEEE 802.1x.

Examples

The following example shows how to set accounting exec:

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa accounting exec default start-stop tacacs-plus none
```

Related Commands

11.5 aaa accounting commands

Set authentication, authorization, accounting (AAA) accounting at login.

Command Syntax

aaa accounting commands (default|LISTNAME) ((tacacs-plus (none)) | none)

no aaa accounting commands (default|LISTNAME)

default	Default method list
<i>LISTNAME</i>	An accounting list with this name
none	No accounting
tacacs-plus	TACACS+

Command Mode

Global Configuration

Default

None

Usage

Use the aaa accounting commands global configuration command to specify one or more AAA accounting methods for use on ports running IEEE 802.1x.

Examples

The following example shows how to set accounting commands:

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa accounting commands default tacacs-plus none
```

Related Commands

11.6 aaa privilege mapping

Set the mapping range in AAA server and switch.

Command Syntax

aaa privilege mapping <0-12> <0-13> <0-14>

no aaa privilege mapping

<i><0-12></i>	The max server privilege mapping to switch level 1
<i><0-13></i>	The max server privilege mapping to switch level 2
<i><0-14></i>	The max server privilege mapping to switch level 3

Command Mode

Global Configuration

Default

0: The server privilege 0 mapping to switch level 1

1: The server privilege 1 mapping to switch level 2

9: The server privilege 2~9 mapping to switch level 3

Other: The server privilege 10~15 mapping to switch level 4

Usage

Use the `aaa privilege mapping` global configuration command to set the mapping range in AAA server and switch.

Examples

The following example shows how to set accounting commands:

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa privilege mapping 0 1 14
```

Related Commands

11.7 login authentication

Enable authentication, authorization, accounting (AAA) authentication for logins.

Command Syntax

login authentication (**default**|*LISTNAME*)

no login authentication

default	Default method list
<i>LISTNAME</i>	An authentication list with this name

Command Mode

Line Configuration mode

Default

None

Usage

None

Examples

The following example shows how to enable authentication for logins:

```
Switch# configure terminal
Switch(config)# line vty 0 7
Switch(config-line)# login authentication default
```

Related Commands

show aaa method-lists authentication

11.8 authorization exec

Enable authentication, authorization, accounting (AAA) authorization for logins.

Command Syntax

authorization exec (default|*LISTNAME*)

no authorization exec

default	Default method list
<i>LISTNAME</i>	An authorization list with this name

Command Mode

Line Configuration mode

Default

None

Usage

None

Examples

The following example shows how to enable authorization for logins:

```
Switch# configure terminal
Switch(config)# line vty 0 7
Switch(config-line)# authorization exec default
```

Related Commands

11.9 accounting exec

Enable authentication, authorization, accounting (AAA) accounting for logins.

Command Syntax

accounting exec (default|*LISTNAME*)

no accounting exec

default	Default method list
<i>LISTNAME</i>	An accounting list with this name

Command Mode

Line Configuration mode

Default

None

Usage

None

Examples

The following example shows how to enable accounting for logins:

```
Switch# configure terminal
Switch(config)# line vty 0 7
Switch(config-line)# accounting exec default
```

Related Commands

11.10 accounting commands

Enable authentication, authorization, accounting (AAA) accounting for logins.

Command Syntax

accounting commands (default|LISTNAME)

no accounting commands

default	Default method list
<i>LISTNAME</i>	An accounting list with this name

Command Mode

Line Configuration mode

Default

None

Usage

None

Examples

The following example shows how to enable accounting for logins:

```
Switch# configure terminal
Switch(config)# line vty 0 7
Switch(config-line)# accounting commands default
```

Related Commands

11.11 show aaa method-lists authentication

Use this command to show authentication, authorization, accounting (AAA) authentication method lists.

Command Syntax

show aaa method-lists authentication

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to show authentication, authorization, accounting (AAA) authentication method lists.

Examples

The following example shows how to show authentication method lists:

```
Switch# show aaa method-lists authentication
authen queue = AAA_ML_AUTHEN_LOGIN
  name = default state = ALIVE : radius
authen queue = AAA_ML_AUTHEN_LOGIN
  name = group_a state = ALIVE : radius local line enable none
authen queue=AAA_ML_AUTHEN_LOGIN
  name = group_b state = ALIVE : local line none
```

Related Commands

aaa authentication login

11.12 show aaa status

Use this command to show authentication, authorization, accounting (AAA) status.

Command Syntax

show aaa status

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to show authentication, authorization, accounting (AAA) status.

Examples

The following example shows how to show authentication, authorization, accounting status:

```
Switch# show aaa status
aaa stats:
  Authentication enable
```

Related Commands

aaa new-model

11.13 show aaa privilege mapping

Use this command to show privilege mapping relationship with server privilege.

Command Syntax

```
show aaa privilege mapping
```

Command Mode

Privileged EXEC

Default

None

Usage

This command to show privilege mapping relationship with server privilege.

Examples

The following example shows how to show authentication method lists:

```
Switch# show aaa privilege mapping
  Server      Switch      Server
=====
      0         1         0
      1         2         1
     2~10      3         10
    11~15     4         15
```

Related Commands

aaa privilege mapping

12 Tacacs+ Commands

12.1 tacacs-server host

Specifies and defines the IP address of the TACACS+ server host.

Command Syntax

tacacs-server host (**mgmt-if**) *A.B.C.D* [**single-connection** | **port** *integer* | **timeout** *integer* | **key string**]

no tacacs-server host (**mgmt-if**) *A.B.C.D* [**single-connection** | **port** *integer* | **timeout** *integer* | **key string**]

mgmt-if	Management port
<i>A.B.C.D</i>	TACACS+ server IP address
single-connection	Maintains a single open connection
port <i>integer</i>	TACACS server port number (default 49)
timeout <i>integer</i>	Time to wait for a TACACS server to reply
key string	Set TACACS+ encryption key

Command Mode

Global Configuration

Default

None

Usage

Add or delete a TACACS+ server host.

Examples

The following example shows how to specify a TACACS+ server host:

```
Switch# configure terminal
Switch(config)# tacacs-server host 10.10.10.1 port 55 key my_key
```

Related Commands

show tacacs

12.2 clear tacacs statistics

To reset statistics on TACACS+ servers, use the clear tacacs statistics EXEC command.

Command Syntax

clear tacacs statistics

Command Mode

Privileged EXEC

Default

None

Usage

Reset statistics on TACACS+ servers.

Examples

The following example shows how to reset statistics on TACACS+ servers:

```
Switch# clear tacacs statistics
```

Related Commands

show tacacs

12.3 show tacacs

To display statistics for a TACACS+ server, use the show tacacs command in EXEC configuration mode.

Command Syntax

show tacacs

Command Mode

Privileged EXEC

Default

None

Usage

This command is used to show TACACS+ servers statistics.

Examples

The following example shows how to show TACACS+ servers:

```
Switch# show tacacs
Tacacs+ Server      : 1.2.3.4/49
  Socket opens:      1
  Socket closes:     0
  Socket aborts:     0
  Socket errors:     0
  Socket Timeouts:   0
Failed Connect Attempts: 0
Total Packets Sent:  2
Total Packets Recv:  2
```

Field	Description
Tacacs+ Server	IP address of the TACACS+ server
Socket opens	Number of successful TCP socket connections to the TACACS+ server
Socket closes	Number of successfully closed TCP socket attempts
Socket aborts	Number of premature TCP socket closures to the TACACS+ server; that is, the peer did not wait for a reply from the server after a the peer sent its request
Socket errors	Any other socket read or write errors, such as incorrect packet format and length
Failed Connect Attempts	Number of failed TCP socket connections to the TACACS+ server.
Total Packets Sent	Number of packets received from the TACACS+ server
Total Packets Recv	Number of outstanding replies from the TACACS+ server

Related Commands

tacacs-server host

13

Port Isolate Commands

13.1 port-isolate group

Use the port-isolate group interface configuration command on the switch to set the isolate group of a interface.

Use the no form of this command to return to the default setting.

Command Syntax

port-isolate group *group*

no port-isolate group

<i>group</i>	Port isolate group id, range is 1-30
--------------	--------------------------------------

Command Mode

Interface Configuration

Default

None

Usage

The ports in the same isolate-group can not communicate with each other.

The ports in different isolate-groups should not be affected by this feature.

The isolate-groups can only be configured on physical port and Link Aggregation.

Examples

The following is sample output from the port-isolate group command:

```
Switch(config-if)# port-isolate group 4
```

Related Commands

port-isolate mode

13.2 port-isolate mode

Use the port-isolate mode global configuration command on the switch to set isolate mode.

Use the no form of this command to return to the default setting.

Command Syntax

port-isolate mode (all | 12)

no port-isolate mode

all	Isolate bridged packets and routed packets
l2	Isolate bridged packets

Command Mode

Global Configuration

Default

None

Usage

If configure “port-isolate mode l2”, all routed packets should not obey the port isolate rules.

If configure “port-isolate mode all”, all packets should obey the port isolate rules.

The default setting is “l2”

Examples

The following is sample output from the port-isolate mode command:

```
Switch(config)# port-isolate mode all
```

Related Commands**port-isolate group**

13.3 show port-isolate

Use the show port-isolate command on the switch to check the port-isolate configuration.

Command Syntax**show port-isolate (group *isolate-group-id*)**

group <i>isolate-group-id</i>	Port isolate group id (1-30)
--------------------------------------	------------------------------

Command Mode

EXEC

Default

None

Usage

None

Examples

The following is sample output from the show port-isolate command:

```
switch # show port-isolate group 12  
Port Isolate Mode : L2
```

```
-----  
Port Isolate Groups:  
-----
```

```
Groups ID: 12
```

```
eth-0-1  eth-0-2  eth-0-3  eth-0-4  eth-0-5
```

```
eth-0-6  
-----
```

Related Commands

port-isolate group

14 Private Vlan Commands

14.1 switchport mode private-vlan

To configure the switch port's mode as private vlan, use the “switchport mode private-vlan” command in interface mode.

Command Syntax

switchport mode private-vlan (*host* | *promiscuous*)

<i>host</i>	Set the port as private vlan, host port
<i>promiscuous</i>	Set the port as private vlan, promiscuous port

Command Mode

Interface mode

Default

By default the switch port's mode is access vlan.

Usage

To configure the switch port's mode as private vlan, use the “switchport mode private-vlan” command in interface mode.

This can only be configured on a switchport.

Examples

```
Switch(config)# interface eth-0-1
Switch (config-if)# switchport mode private-vlan host
Switch (config-if)# switchport mode private-vlan promiscuous
```

Related Commands

switchport private-vlan

14.2 switchport private-vlan

To configure the primary and secondary vlan of a private vlan, use the “switchport private-vlan” command in interface mode.

Use the “no” form of this command to restore the default value.

Command Syntax

switchport private-vlan <1-4094> (**isolate** | **community-vlan** <1-4094> |)

private-vlan <1-4094>	Set private primary vlan
isolate	Set as isolate mode
community-vlan <1-4094>	Set communtiy vlan

Command Mode

Interface mode

Default

By default, the primary vlan is 1.

If the switchport mode is private-vlan host, the default mode is isolate; Or else the switchport mode is promiscuous

Usage

To configure the primary and secondary vlan of a private vlan, use the “switchport private-vlan” command in interface mode.

This can only be configured on a switchport.

Examples

```
Switch (config)# interface eth-0-1
Switch (config-if)# switchport mode private-vlan host
Switch (config-if)# switchport private-vlan 1 isolate
Switch (config-if)# quit
Switch (config)# interface eth-0-2
Switch (config-if)# switchport mode private-vlan host
Switch (config-if)# switchport private-vlan 1 community-vlan 2
Switch (config-if)# quit
Switch (config)# interface eth-0-3
Switch (config-if)# switchport mode private-vlan promiscuous
Switch (config-if)# switchport private-vlan 1
```

Related Commands

switchport mode private-vlan

14.3 show private-vlan

To display the private-vlan configure, use the show private-vlan command in privileged EXEC mode.

Command Syntax

show private-vlan (vlan <1-4094> | interface IFPHYSICAL | interface IFAGG |)

vlan <1-4094>	Show by primary vlan
interface IFPHYSICAL interface IFAGG	Show by interface

Command Mode

Privileged EXEC

Default

N/A

Usage

无

Examples

```
Switch# show private-vlan
Primary  Secondary Type      Ports
-----
1        N/A      promiscuous eth-0-3
1        N/A      isolate     eth-0-1
1        2        community   eth-0-2
```

```
DUT1# show private-vlan vlan 1
Primary  Secondary Type      Ports
-----
1        N/A      promiscuous eth-0-3
1        N/A      isolate     eth-0-1
1        2        community   eth-0-2
```

```
DUT1# show private-vlan interface eth-0-1
-----
Private vlan mode: isolate
Primary vlan id : 1
```

Related Commands

switchport mode private-vlan

switchport private-vlan

15 DDOS Commands

15.1 ip icmp intercept

To configure the system to resist ICMP flood attack, use the `ip icmp intercept` command in global configuration mode. To disable this capability, use the `no` form of this command.

Command Syntax

ip icmp intercept [maxcount *number*]

no ip icmp intercept

maxcount	Specify max counter of received packet rate
<i>number</i>	Number of received packets per second, the range is 0-1000, default value is 500

Command Mode

Privileged EXEC

Default

By default, `ip icmp intercept` is unset.

Usage

Use this command if you want to set the system to limit the ICMP packet rate.

Examples

The following example shows how to configure the `ip icmp intercept`:

```
Switch(config)# ip icmp intercept maxcount 100
```

The following example unsets the `ip icmp intercept`:

```
Switch(config)# no ip icmp intercept
```

Related Commands

show ip-intercept config

15.2 ip smurf intercept

To configure the system to resist smurf attack, use the `ip smurf intercept` command in global configuration mode. To disable this capability, use the `no` form of this command.

Command Syntax

[no] ip smurf intercept

Command Mode

Global Configuration

Default

By default, ip smurf intercept is unset.

Usage

Use this command if you want to set the system to resist smurf attack.

Examples

The following example shows how to configure the ip smurf intercept:

```
Switch(config)# ip smurf intercept
```

The following example unset the ip smurf intercept:

```
Switch(config)# no ip smurf intercept
```

Related Commands

show ip-intercept config

15.3 ip fraggle intercept

To configure the system to resist fraggle attack, use the ip fraggle intercept command in global configuration mode. To disable this capability, use the no form of this command.

Command Syntax

ip fraggle intercept

no ip fraggle intercept

Command Mode

Global configuration

Default

By default, ip fraggle intercept is unset.

Usage

Use this command if you want to set the system to resist fraggle attack.

Examples

The following example shows how to configure the ip fraggle intercept:

```
Switch(config)# ip fraggle intercept
```

The following example unset the ip fraggle intercept:

```
Switch(config)# no ip fraggle intercept
```

Related Commands

show ip-intercept config

15.4 ip udp intercept

To configure the system to resist UDP flood attack, use the ip udp intercept command in global configuration mode. To disable this capability, use the no form of this command.

Command Syntax

ip udp intercept [maxcount *number*]

no ip udp intercept

maxcount	Specify max counter of received packet rate
<i>number</i>	Number of received packets per second, the range is 0-1000, default value is 500

Command Mode

Global Configuration

Default

By default, ip udp intercept is unset.

Usage

Use this command if you want to set the system to limit the UDP packet rate.

Examples

The following example shows how to configure the ip udp intercept:

```
Switch(config)# ip udp intercept maxcount 100
```

The following example unset the ip udp intercept:

```
Switch(config)# no ip udp intercept
```

Related Commands

show ip-intercept config

15.5 ip tcp intercept

To configure the system to resist SYN flood attack, use the ip tcp intercept command in global configuration mode. To disable this capability, use the no form of this command.

Command Syntax

ip tcp intercept (maxcount *number* |)

no ip tcp intercept

maxcount	Specify max counter of received packet rate
<i>number</i>	Number of received packets per second, the range is 0-1000, default value is 500

Command Mode

Global Configuration

Default

By default, ip tcp intercept is unset.

Usage

Use this command if you want to set the system to limit the TCP packet rate with only SYN bit set.

Examples

The following example shows how to configure the ip tcp intercept:

```
Switch(config)# ip tcp intercept maxcount 100
```

The following example unset the ip tcp intercept:

```
Switch(config)# no ip tcp intercept
```

Related Commands

show ip-intercept config

15.6 ip small-packet intercept

To configure the system to filter the small packet, use the ip small-packet command in global configuration mode. To disable this capability, use the no form of this command.

Command Syntax

ip small-packet intercept (length *number* |)

no ip small-packet intercept

length	Specify length of small packet
<i>number</i>	Length of received packets, the range is 28-65535, default value is 28

Command Mode

Global Configuration

Default

By default, ip small-packet intercept is unset.

Usage

Use this command if you want to set the system to drop the packet which length is less than the configured value.

Examples

The following example configures the ip small-packet intercept:

```
Switch(config)# ip small-packet intercept length 32
```

The following example unset the ip small-packet intercept:

```
Switch(config)# no small-packet intercept
```

Related Commands

show ip-intercept config

15.7 ip maceq intercept

To configure the system to intercept the packet whose source MAC equals to destination MAC, use the ip maceq intercept command in global configuration mode. To disable this capability, use the no form of this command.

Command Syntax

ip maceq intercept

no ip maceq intercept

Command Mode

Global Configuration

Default

By default, ip maceq intercept is unset.

Usage

Use this command if you want to set the system to drop the packet whose source MAC equals to destination MAC.

Examples

The following example configures the ip intercept maceq:

```
Switch(config)# ip maceq intercept
```

The following example unset the ip intercept maceq:

```
Switch(config)# no ip maceq intercept
```

Related Commands

show ip-intercept config

15.8 ip ipeq intercept

To configure the system to intercept the packet whose source IP address equals to destination IP address, use the ip ipeq intercept command in global configuration mode. To disable this capability, use the no form of this command.

Command Syntax

ip ipeq intercept

no ip ipeq intercept

Command Mode

Global Configuration

Default

By default, ip ipeq intercept is unset.

Usage

Use this command if you want to set the system to drop the packet whose source IP address equals to destination IP address.

Examples

The following example configures the ip intercept ipeq:

```
Switch(config)# ip ipeq intercept
```

The following example unset the ip intercept ipeq:

```
Switch(config)# no ip ipeq intercept
```

Related Commands

show ip-intercept config

15.9 show ip-intercept config

To display the ip intercept configurations, use the show ip-intercept config command in privileged EXEC mode.

Command Syntax

show ip-intercept config

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to display ip intercept configurations.

Examples

The following example shows the configuration of ip intercept:

```
Switch# show ip-intercept config
Current DDoS Prevent configuration:
=====
ICMP Flood Intercept      :Enable  Maxconut:100
UDP Flood Intercept      :Enable  Maxconut:100
SYN Flood Intercept      :Enable  Maxconut:100
Small-packet Attack Intercept  :Enable  Packet Length:32
Sumrf Attack Intercept   :Enable
Fraggle Attack Intercept :Enable
MAC Equal Intercept      :Disable
IP Equal Intercept       :Disable
```

Related Commands

show ip-intercept config

15.10 show ip-intercept config

To display the ip intercept configurations, use the show ip-intercept config command in privileged EXEC mode.

Command Syntax

show ip-intercept config

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to display ip intercept configurations.

Examples

The following example shows the configuration of ip intercept:

```
Switch# show ip-intercept config
Current DDoS Prevent configuration:
=====
ICMP Flood Intercept      :Enable  Maxconut:100
```

```
UDP Flood Intercept      :Enable Maxconut:100
SYN Flood Intercept      :Enable Maxconut:100
Small-packet Attack Intercept  :Enable Packet Length:32
Sumrf Attack Intercept   :Enable
Fraggle Attack Intercept  :Enable
MAC Equal Intercept      :Disable
IP Equal Intercept       :Disable
```

Related Commands

show ip-intercept config

15.11 show ip-intercept statistics

To display the statistics of the intercept packets, use the show ip-intercept statistics command in privileged EXEC mode.

Command Syntax

show ip-intercept statistics

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to display ip intercept statistics.

Examples

The following is sample output from the show ip-intercept statistics command:

```
Switch# show ip-intercept statistics
Current DDoS Prevent statistics:
=====
Resist Small-packet Attack packets number   : 108
Resist ICMP Flood packets number            : 0
Resist Smurf Attack packets number          : 0
Resist SYN Flood packets number            : 0
Resist Fraggle Attack packets number       : 0
Resist UDP Flood packets number            : 0
```

Related Commands

clear ip-intercept statistics

15.12 clear ip-intercept statistics

To clear the statistics of the intercept packets, use the clear ip-intercept statistics command in privileged EXEC mode.

Command Syntax

clear ip-intercept statistics

Command Mode

Privileged EXEC

Default

None

Usage

Use this command to clear ip intercept statistics.

Examples

The following example displays how to use clear ip-intercept statistics command:

```
Switch# clear ip-intercept statistics
Switch# show ip-intercept statistics
Current DDoS Prevent statistics:
=====
Resist Small-packet Attack packets number    : 0
Resist ICMP Flood packets number             : 0
Resist Smurf Attack packets number           : 0
Resist SYN Flood packets number              : 0
Resist Fraggle Attack packets number         : 0
Resist UDP Flood packets number              : 0
```

Related Commands

show ip-intercept statistics

16 Key Chain Commands

16.1 key chain

To create a keychain, use the key chain command in global configuration mode. To delete a keychain, use the no form of this command.

Command Syntax

key chain *WORD*

no key chain *WORD*

<i>WORD</i>	The name of keychain
-------------	----------------------

Command Mode

Global Configuration

Default

No keychain is created.

Usage

Routing protocols and network management applications often use keychain to enhance security while communicating with peers. For the detail of these configurations, see relevant chapters of user guide.

Examples

The following example shows how to create a keychain:

```
Switch(config)# key chain test
```

Related Commands

key

key-string

show key chain

16.2 key

To create a key in a keychain, use the key command in keychain configuration mode. To delete a key from a keychain, use the no form of this command.

Command Syntax

key <0-31>

no key <0-31>

Command Mode

Keychain configuration

Default

There is no key in a keychain.

Usage

The key will not be used unless key string was configured.

Examples

The following example shows how to create a key:

```
Switch(config-keychain)# key 1
```

Related Commands

key chain

key-string

accept-lifetime

send-lifetime

16.3 key-string

To configure key string for a key, use key-string command in key configuration mode. To delete configuration, use the no form of this command.

Command Syntax

key-string *LINE*

no key-string *LINE*

<i>LINE</i>	Key string and the length range is 0~255
-------------	--

Command Mode

Key configuration

Default

The key string is not be configured.

Usage

This command is used to configure key string for a key and then this key will be valid for ever if there is no lifetime set.

Examples

The following example shows how to configure key-string:

```
Switch(config-keychain-key)# key-string ##test_keywords##
```

Related Commands

key

accept-lifetime

send-lifetime

16.4 accept-lifetime

To configure the accept lifetime for a key, use `accept-lifetime` command in key configuration mode. To delete this configuration, use the `no` form of this command.

Command Syntax

accept-lifetime *START-TIME EXPIRE-TIME*

no accept-lifetime

<i>START-TIME</i>	The start of accept lifetime,its format should like "HH:MM:SS <1-31> MONTH <1993-2035>" or "HH:MM:SS MONTH <1-31> <1993-2035>" and MONTH should be First three letters of the month
<i>EXPIRE-TIME</i>	The end of accept lifetime,its format should like "HH:MM:SS <1-31> MONTH <1993-2035>", "HH:MM:SS MONTH <1-31> <1993-2035>", "Infinite" or "duration <1-2147483646>" and MONTH should be First three letters of the month

Command Mode

Key configuration

Default

No accept lifetime is configured

Usage

This command is used to configure accept lifetime for a key which will be invalid after lifetime expired.

Examples

The following example shows how to configure accept-lifetime:

```
Switch(config-keychain-key)# accept-lifetime 0:0:1 2 jan 2012 infinite
```

Related Commands

key

key-string

16.5 send-lifetime

To configure the send lifetime for a key, use `send-lifetime` command in key configuration mode. To delete this configuration, use the `no` form of this command.

Command Syntax

send-lifetime *START-TIME EXPIRE-TIME*

no send-lifetime

<i>START-TIME</i>	The start of send lifetime,its format should like "HH:MM:SS <1-31> MONTH <1993-2035>" or "HH:MM:SS MONTH <1-31> <1993-2035>" and MONTH should be First three letters of the month
<i>EXPIRE-TIME</i>	The end of send lifetime,its format should like "HH:MM:SS <1-31> MONTH <1993-2035>", "HH:MM:SS MONTH <1-31> <1993-2035>", "Infinite" or "duration <1-2147483646>" and

	MONTH should be First three letters of the month
--	--

Command Mode

Key configuration

Default

No send lifetime is configured

Usage

This command is used to configure send lifetime for a key which will be invalid after lifetime expired.

Examples

The following example shows how to configure send-lifetime:
Switch(config-keychain-key)# send-lifetime 0:0:1 2 jan 2012 infinite

Related Commands

key

key-string

16.6 show key chain

To show information of keychain, use show key chain command.

Command Syntax

show key chain (*WORD*)

<i>WORD</i>	The name of keychain
-------------	----------------------

Command Mode

Privileged EXEC

Default

None

Usage

None

Examples

The following example shows how to display keychain:

```
Switch# show key chain test
key chain test:
  key 1 -- text "key-string ##test_keywords_1##"
    accept-lifetime <00:00:01 Jan 01 2012> - <infinite>
    send-lifetime <always valid> - <always valid> [valid now]
  key 2 -- text "key-string ##test_keywords_2##"
    accept-lifetime <always valid> - <always valid> [valid now]
    send-lifetime <00:00:01 Jan 02 2012> - <infinite>
```

Related Commands

key chain

key

key-string

17

Port-block Commands

17.1 port-block

To configure, use the port-block command in interface configuration mode. To delete this configuration, use the no form of this command.

Command Syntax

port-block (known-unicast | known-multicast | unknown-unicast | unknown-multicast | broadcast)

no port-block (known-unicast | known-multicast | unknown-unicast | unknown-multicast | broadcast)

known-unicast	Specify that known unicast traffic should be blocked
known-multicast	Specify that known multicast traffic should be blocked
unknown-unicast	Specify that unknown unicast traffic should be blocked
unknown-multicast	Specify that unknown multicast traffic should be blocked
broadcast	Specify that broadcast traffic should be blocked

Command Mode

Interface Configuration Mode

Default

Unknown or known multicast and unicast traffic is not blocked.

Broadcast traffic is not blocked.

Usage

By default, all traffic with unknown MAC addresses is sent to all ports. You can block unknown multicast or unicast traffic on protected or non protected ports. If unknown multicast or unicast traffic is not blocked on a protected port, there could be security issues.

With multicast traffic, the port blocking feature blocks only pure Layer 2 packets. Multicast packets that contain IPv4 or IPv6 information in the header are not blocked.

Examples

This example shows how to block unknown multicast traffic on an interface:

```
Switch(config-if) # port-block known-unicast
```

Related Commands

show port-block (interface IFPHYSICAL | interface IFAGG)

17.2 show port-block

Display the port-block configuration in interface configuration mode.

Command Syntax

show port-block (interface IFPHYSICAL | interface IFAGG)

IFPHYSICAL	Specify the physical interface
IFAGG	Specify the aggregation interface

Command Mode

Privileged EXEC

Default

N/A

Usage

Display the port-block configuration in interface configuration mode..

Examples

This example shows how to show port-block configuration in Privileged EXEC mode:

```
Switch# show port-block interface eth-0-1
```

Related Commands

port-block (known-unicast | known-multicast | unknown-unicast | unknown-multicast | broadcast)