Network Protocol CLI Reference Guide

Model: S3700-24T4F

CLI REFERENCE GUIDE

Table of Contents

1.1 IP Address Configuration Commands 1
1.1.1 arp 1
1.1.2 arp max-gw-retries 2
1.1.3 arp retry-allarp 3
1.1.4 arp timeout 4
1.1.5 arp send-gratuitous 5
1.1.6 clear arp-cache 5
1.1.7 ip address 6
1.1.8 ip host 7
1.1.9 show arp 8
1.1.10 show hosts 9
1.1.11 show ip interface 9
Chapter 2 DHCP Client Configuration Commands 12
2.1 DHCP Client Configuration Commands 12
2.1.1 ip address dhcp 12
2.1.2 ip dhcp client 13
2.1.3 ip dhcp-server 15
2.1.4 show dhcp lease 16
2.1.5 show dhcp server 17
2.1.6 debug dhcp 18
Chapter 3 IPv6 Configuration Commands 19
3.1 IP Service Configuration Commands 19
3.1.1 clear tcp 19
3.1.2 clear tcp statistics 21
3.1.3 debug arp 21
3.1.4 debug ip icmp 23
3.1.5 debug ip packet 27
3.1.6 debug ip raw 31
3.1.7 debug ip tcp packet 33
3.1.8 debug ip tcp transactions 34
3.1.9 debug ip udp 37
3.1.10 ip mask-reply 38
3.1.11 ip mtu 38
3.1.12 ip source-route 39
3.1.13 ip tcp synwait-time 40
3.1.14 ip tcp window-size 41
3.1.15 ip unreachables 41
3.1.16 show ip sockets 42
3.1.17 show ip traffic 43
3.1.18 show tcp 45

3.1.19 show tcp brief 50
3.1.20 show tcp statistics 51
3.1.21 show tcp tcb 53
3.2 ACL Configuration Commands 54
3.2.1 deny 54
3.2.2 ip access-group 57
3.2.3 ip access-list 58
3.2.4 permit 59
3.2.5 show ip access-list 61
3.3 IP ACL based on physical port 62
3.3.1 deny 63
3.3.2 ip access-group 65
3.3.3 ip access-list 66
3.3.4 permit 67
3.3.5 show ip access-list 69

Chapter 1 IP Address Configuration Commands

1.1 IP Address Configuration Commands

IP Address Configuration Commands include:

- arp arp
- arp max-gw-retries
- arp retry-allarp
- arp send-gratuitous
- arp timeout
- clear arp-cache
- ip address
- ip host
- show arp
- show hosts
- show ip interface

1.1.1 arp

Syntax

To add a static and permanent entry in the Address Resolution Protocol (ARP) cache, use the arp command in global configuration mode. To remove an entry from the ARP cache, use the no form of this command.
arp *ip-address hardware-address vlan* [**alias**]
no arp *ip-address [vlan]*

Parameters

Parameters	Description
ip-address	IP address corresponding to the local data-link address.
hardware-address	Physical address of local data-link address
vlan	The vlan interface belongs to the static arp
alias	(optional) switch responds to ARP requests as if it were the interface of the specified address.

Default Value

No entries are permanently installed in the ARP cache.

Command Mode

Global configuration mode

Usage Guidelines

The common host all supports dynamic ARP analysis, so user doesn't need to configure static ARP entries for host.
Usually to delete static arp, run no arp *ip_address vlan*. If the vlan interface belongs to a static arp is deleted, delete the static arp by running no arp *ip_address*.

Example

The following example shows that the MAC address of the host with IP address 1.1.1.1 is set to 00:12:34:56:78:90.

```
arp 1.1.1.1 00:12:34:56:78:90   vlan1
```

Related Command

clear arp-cache

1.1.2 arp max-gw-retries

Syntax

To set the maximum retransmissions of the Re-Detect packets, run the following command. To return to the default setting, use the no form of this command.
arp max-gw-retries *number*
no arp max-gw-retries

Parameters

Parameters	Description
number	Sets the maximum retransmissions of the Re-Detect packets.

Default Value

3

Command Mode

Global configuration mode

Usage Guidelines

The ARP entries, which the routing entry gateway depends on, require being redetected at their aging so that the promptness and correctness of the hardware subnet routing can be guaranteed. This command is here used for setting the maximum ARP retransmissions in the redetection process. The bigger its value is, the greater chance the detection has.

Example

The following example shows how to set the maximum retransmissions of the Re-Detect packets to 5:

arp max-gw-retries 5

Related Command

show arp

1.1.3 arp retry-allarp

Syntax

To set whether to carry on redetection at the aging of ARP entries (not just meaning the gateway-related ARP entries), run the following command:
arp retry-allarp
no arp retry-allarp

Parameters

None

Command Mode

Global configuration mode

Usage Guidelines

By default, redetection is conducted only to the aging ARPs, which the routing entry gateway depends on. However, if this command is enabled, redetection will be conducted towards all types of aging ARP entries.

Example

The following example shows how to enable redetection to be carried out to all aging ARP entries.

arp retry-allarp

Related Command

show arp

1.1.4 arp timeout

Syntax

To configure the exist time that a dynamic ARP entry remains in the Address Resolution Protocol (ARP) cache, use the arp timeout. To restore the default value, use the no form of this command or default arp timeout command.
arp timeout *seconds*
no arp timeout
default arp timeout

Parameters

Parameters	Description
seconds	Time in seconds that an entry remains in the ARP cache. A value of zero means that entries are never cleared from the cache.

Default Value

14400 seconds (4 hours)

Command Mode

Interface configuration mode

Usage Guidelines

This command is ignored when it is not configured on interfaces using ARP. The show interface command displays the ARP timeout value, as seen in the following example from the show interfaces command:
ARP type: ARPA, ARP timeout 04:00:00

Example

The following example sets the ARP timeout to 900 seconds on interface vlan 10 to allow entries to time out more quickly than the default.

```
interface vlan 10
arp timeout 900
```

Related Command

show interface

1.1.5 arp send-gratuitous

Syntax

To configure ARP send-gratuitous function, use the arp send-gratuitous command.
arp send-gratuitous [**interval** *value*]
no arp send-gratuitous

Parameters

Parameters	Description
interval	Set the intervals of arp send-gratuitous
value	Set time interval, the default is 120 seconds. The range is 15 to 600 seconds

Command Mode

Port configuration mode

Example

The following example start arp send-gratuitous on Interface Vlan 1, and set the send interval as 3 minutes.

switch_config_v1#arp send-gratuitous interval 180

Related Command

arp

1.1.6 clear arp-cache

Syntax

To clear all dynamic entries from the ARP cache, use the clear arp-cache command.
clear arp-cache [*ip-address* [*mask* | *vlan vlanid*]]

Parameters

Parameters	Description
ip-address	IP or subnets

mask	Subnet mask
vlanid	vlan ID

Command Mode

EXEC

Example

The following example shows how to clear all dynamic ARP cache.

clear arp-cache

Related Command

arp

1.1.7 ip address

Syntax

To set an IP address and mask for an interface, use the ip address command. Currently, there is no strict regulation to distinguish A.B.C IP address. But multicast address and broadcast address can not be used(all host section is '1'). Other than the Ethernet,multiple interfaces of other types can be connected to the same network. Other than the unnumbered interface, the configured network range of the Ethernet interface can not be the same as the arbitrary interfaces of other types. Usually one interface usually can configure one master address and numerous secondary addresses. You should configure the primary address before configuring the secondary address. IP packets generated by the system, if the upper application does not specify the source address, the switch will use the IP address configured on the sending interface that on the same network range with the gateway as the source address of the packet. If the IP address is uncertain (like interface route), the switch will use the primary address of the sending interface. If the ip address is not configured on an interface, also it is not the unnumbered interface, and then this interface will not deal with any IP packet.

To remove an IP address or disable IP processing, use the no form of this command.

ip address *ip-address mask* [secondary]

no ip address *ip-address mask*

no ip address

Parameters

Parameters	Description
ip-address	IP address
mask	Mask of the IP network

secondary	(optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.

Default Value

No IP address is defined for the interface.

Command Mode

Interface configuration mode

Usage Guidelines

If any switch on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet.
When you are routing using the Open Shortest Path First (OSPF) algorithm, ensure that all secondary addresses of an interface fall into the same OSPF area as the primary addresses.

Example

In the following example, 202.0.0.1 is the primary address, 255.255.255.0 is the mask and 203.0.0.1 and 204.0.0.1 are secondary addresses for EthernetVLAN 10.

interface vlan 10

ip address 202.0.0.1 255.255.255.0

ip address 203.0.0.1 255.255.255.0 secondary

ip address 204.0.0.1 255.255.255.0 secondary

1.1.8 ip host

Syntax

To define the name-address mapping of the static host, run ip host name hostname address. To delete the name-address mapping of the static host, run no ip host name hostname.
ip host *name address*
no ip host *name*

Parameters

Parameters	Description
name	Name of the host
Address	IP address

Default Value

No mapping is configured.

Command Mode

Global configuration mode

Example

The following example shows how to set the name of the host with IP address 202.96.1.3 to dns-server.

ip host dns-server 202.96.1.3

1.1.9 show arp

Syntax

To display the entries in the Address Resolution Protocol (ARP) table, including the ARP mapping of interface IP address, the static ARP mapping that user configures and the dynamic ARP mapping, use the show arp command.

show arp

Parameters

The command has no parameters or keywords.

Command Mode

EXEC

Usage Guidelines

Shown information include:

Protocol	Protocol, the type of physical address mapping, for instance, IP.
Address	Address, the network address mapping the physical address, for instance, IP address.
Age	Time to Live, from generating ARP entries to now. Unit: min. The value will not be affected if the switch uses the ARP entry.
Hardware Address	physical address, the address corresponding to the network address. The entry has not resolved is empty.
Type	Type, means the encapsulation type the interface uses, such as ARPA and SNAP.
Interface	Interface, the interface connects to the network address.

Example

The following example shows ARP cache

switch#show arp

Protocol	IP Address	Age(min)	Hardware Address	Type	Interface
IP	192.168.20.77	11	00:30:80:d5:37:e0	ARPA	vlan 10
IP	192.168.20.33	0	Incomplete		
IP	192.168.20.22	-	08:00:3e:33:33:8a	ARPA	vlan 10
IP	192.168.20.124	0	00:a0:24:9e:53:36	ARPA	vlan 10
IP	192.168.0.22	-	08:00:3e:33:33:8b	ARPA	vlan 11

1.1.10 show hosts

Syntax

To show all entries in host name-address cache, run this command.
show hosts

Parameters

The command has no parameters or keywords.

Command Mode

EXEC

Example

The command shows all host name/address mapping:

show hosts

Related Command

None

1.1.11 show ip interface

Syntax

To show IP configuration of the interface, run this command.
show ip interface [**type** *number* | ***brief***]

Parameters

Parameters	Description
type	(Optional) interface type
number	(Optional) interface number
brief	(Optional) Shows ip protocol brief of all vlan interfaces.

Command Mode

EXEC

Usage Guidelines

If the link layer of an interface can effectively transmit and receive the data, the interface is available, whose state is Protocol Up. If an IP address is configured on the interface, the switch will add an direct-through route to the routing table. If the link-layer protocol is disabled, that is, if the link-layer protocol is Protocol Down, the direct-through route will be deleted. If the interface type and the number of the interface is specified, only the information about the specified interface is displayed. Otherwise, the information about the IP configuration of all interfaces is displayed.

Example

The following example shows the IP configuration of interfaceVLAN 10.

```
switch#show ip interface vlan 10
   vlan 10 is up, line protocol is up
IP address : 192.168.20.167/24
      Broadcast address : 192.168.20.255
      Helper address : not set
      MTU : 1500(byte)
      Forward Directed broadcast : OFF
      Multicast reserved groups joined:
       224.0.0.9 224.0.0.6 224.0.0.5 224.0.0.2
       224.0.0.1
      Outgoing ACL : not set
      Incoming ACL : not set
      IP fast switching : ON
      IP fast switching on the same interface : OFF
      ICMP unreachables : ON
      ICMP mask replies : OFF
```

ICMP redirects : ON

Description

Domain	Description
vlan 10 is up	If the interface hardware is usable, the interface is marked "up." For an interface to be usable, both the interface hardware and line protocol must be up.
line protocol is up	If the interface can provide two-way communication, the line protocol is marked "up." For an interface to be usable, both the interface hardware and line protocol must be up.
IP address	IP address and mask for interface
Broadcast address	Displays broadcast address
MTU	Displays the MTU value set on the interface.
Helper address	Displays helper address
Directed broadcast forwarding	Forwards the directed broadcast packets.
Multicast reserved groups joined	Multicast groups added to the interface
Outgoing ACL	Outgoing access control list used by the interface
Incoming ACL	Incoming access control list used by the interface
IP fast switching	Enables fast switching on the interface by the switch.
Proxy ARP	Enables the proxy ARP on the interface.
ICMP redirects	Forwards the ICMP redirect packet on the interface.
ICMP unreachables	Forwards the ICMP-unreachable packet on the interface.
ICMP mask replies	Forwards the ICMP-mask-replies packet on the interface.

Chapter 2 DHCP Client Configuration Commands

2.1 DHCP Client Configuration Commands

DHCP Client Configuration Commands include:

- ip address dhcp
- ip dhcp client
- ip dhcp-server
- show dhcp lease
- show dhcp server
- debug dhcp

The chapter describes the DHCP configuration commands. These commands are used to configure and monitor the DHCP running on the switch.

2.1.1 ip address dhcp

Syntax

To obtain an IP address for the interface through the dynamic host configuration protocol (DHCP), run this command. To delete the obtained IP address, run no ip address dhcp.

ip address dhcp

no ip address dhcp

Parameters

None

Default Value

None

Command Mode

Interface configuration mode

Usage Guidelines

The ip address dhcp command allows an interface to obtain an IP address through DHCP, which is very useful to dynamically connecting ISP through the Ethernet interface.

When the dynamic IP address is obtained and the ip address dhcp command is configured, the

switch sends the DHCPDISCOVER message to the DHCP server in the network.
When the dynamic IP address is obtained and the no ip address dhcp command is configured, the switch sends the DHCPRELEASE message.

Example

The following example shows that theVLAN11 interface obtains the IP address through the DHCP protocol.

```
!
interface vlan11
 ip address dhcp
```

Related Command

ip dhcp client
ip dhcp-server
show dhcp lease
show dhcp server

2.1.2 ip dhcp client

Syntax

To configure parameters at the DHCP client server of the local switch, run this command.
ip dhcp client { **bootfileaddmac** | **minlease** *seconds* | **retransmit** *count* | **select** *seconds* | **class_identifier** *WORD* | **client_identifier hrd_ether** | **retry_interval** *<1-1440>* | **tftpdownload** | **timeout_shut** }
no ip dhcp client { **bootfileaddmac** | **minlease** | **retransmit** | **select** | **class_identifier** | **client_identifier** | **retry_interval** | **tftpdownload** | **timeout_shut** }

Parameters

Parameters	Description
bootfileaddmac	(optional) Enables bootfile name to add client mac.
minlease *seconds*	Stands for the acceptable minimum lease time, which ranges from 60 to 86400 seconds and an optional parameter.
retransmit *count*	Stands for the retransmission times of the protocol packets, which ranges from 1 to 1o and is an optional parameter.
select *seconds*	(Optional) Stands for the interval of SELECT, which ranges from 5 to 30 and is an optional parameter.
class_identifier *WORD*	(Optional) Sets the class ID belongs to the client
client_identifier hrd_ether	(Optional) Sets the type of client ID to Ethernet

retry_interval *<1-1440>*	(Optional) Sets retry interval
tftpdownload	(Optional) Enable TFTP download function
timeout_shut	(Optional) Enable up/down on the interface when the leasing time outs.

Default Value

The default value of the minlease parameter is 60 seconds.
The default value of the retransmit parameter is 4 times.
The default value of the select parameter is 5 seconds.
class_identifier no parameter default value
client_identifier the parameter default value is the character string
retry_interval the default value is 1 minute
timeout_shut no parameter default value

Command Mode

Global configuration mode.

Usage Guidelines

You can adjust these parameters according the requirements of the network structure and the DHCP server.
If the negative forms of these commands are set, these parameter will resume their default values.

Example

The following example shows how to set the acceptable minimum lease time of the DHCP client on the switch to 100 seconds:

ip dhcp client minlease 100

The following example shows how to set the retransmission times of the protocol packets on the DHCP client of the switch to 3:

ip dhcp client retransmit 3

The following example shows, on the DHCP client of the switch, how to set the interval of SELECT to 10 seconds:

ip dhcp client select 10

Related Command

ip address dhcp
ip dhcp-server
show dhcp lease
show dhcp server

2.1.3 ip dhcp-server

Syntax

To specify a familiar DHCP server, you can use ip dhcp-server to designate the IP address of the DHCP server.
ip dhcp-server *ip-address*
no ip dhcp-server *ip-address*

Parameters

Parameters	Description
ip-address	IP address of the DHCP server

Default Value

There is no default IP address of the DHCP server.

Command Mode

Global configuration mode.

Usage Guidelines

You can designate an IP address for a DHCP server by using this command, which will not replace the previously designated IP address of the DHCP server.
But the previously designated IP address of the DHCP server can be removed by the negative form of this command.

Example

The following example shows how to specify on the swich a server, whose IP address is 192.168.20.1, to be the DHCP server:

```
ip dhcp-server 192.168.20.1
```

Related Command

ip address dhcp
ip dhcp client
show dhcp lease
show dhcp server

2.1.4 show dhcp lease

Syntax

To browse the distribution information of the DHCP server, which is used by the current switch, run show dhcp lease.

Show dhcp lease

Parameters

None

Default Value

None

Command Mode

EXEC

Usage Guidelines

You can use this command to browse the distribution information of the DHCP server of the current switch.

Example

The following example shows how to display the DHCP distribution information of the switch:

```
switch#show dhcp lease
Temp IP addr: 192.168.20.3    for peer on Interface: vlan11
Temp    sub net mask: 255.255.255.0
    DHCP Lease server: 192.168.1.3, state: 4 Rebinding
    DHCP transaction id: 2049
    Lease: 86400 secs,    Renewal: 43200 secs,    Rebind: 75600 secs
Temp default-gateway addr: 192.168.1.2
    Next timer fires after: 02:34:26
    Retry count: 1      Client-ID: router-0030.80bb.e4c0-v11
```

Related Command

ip address dhcp
ip dhcp client
ip dhcp-server

show dhcp server
debug dhcp

2.1.5 show dhcp server

Syntax

To display the known information of the DHCP server, run show dhcp server.
show dhcp server

Parameters

None

Default Value

None

Command Mode

EXEC

Usage Guidelines

This command is used to display the known information of the DHCP server.

Example

The following example shows how to display the already known information about the DHCP server.

```
switch#show dhcp sever
DHCP server: 255.255.255.255
  Leases:    0
  Discovers: 62 Requests: 0       Declines: 0       Releases: 0
  Offers:    0  Acks:     0       Naks:     0       Bad:      0
  Subnet: 0.0.0.0,          Domain name:
```

Related Command

ip address dhcp
ip dhcp client
ip dhcp-server
show dhcp lease

2.1.6 debug dhcp

Syntax

To browse the processing of DHCP when DHCP is run on the switch, run the following command.

debug dhcp [**detail**]
no debug dhcp [**detail**]

Parameters

Parameters	Description
detail	Means to display the content of the DHCP packet.

Default Value

Relative information is not shown.

Command Mode

EXEC

Usage Guidelines

The following example shows some key information about DHCP processing:

switch#debug dhcp

switch#2000-4-22 10:50:40 DHCP: Move to INIT state, xid: 0x7

2000-4-22 10:50:40 DHCP: SDISCOVER attempt # 1, sending 277 byte DHCP packet

2000-4-22 10:50:40 DHCP: B'cast on vlan11 interface from 0.0.0.0

2000-4-22 10:50:40 DHCP: Move to SELECTING state, xid: 0x7

2000-4-22 10:50:46 DHCP: SDISCOVER attempt # 2, sending 277 byte DHCPpacket

2000-4-22 10:50:46 AM DHCP: B'cast on vlan11 interface from 0.0.0.0

2000-4-22 10:50:54 AM DHCP: SDISCOVER attempt # 3, sending 277 byte DHCPpacket

Related Command

show dhcp lease

Chapter 3 IPv6 Configuration Commands

3.1 IP Service Configuration Commands

IP Service Configuration Commands include:

- clear tcp
- clear tcp statistics
- debug arp
- debug ip icmp
- debug ip packet
- debug ip raw
- debug ip tcp packet
- debug ip tcp transactions
- debug ip udp
- ip mask-reply
- ip mtu
- ip source-route
- ip tcp synwait-time
- ip tcp window-size
- ip unreachables
- show ip sockets
- show ip traffic
- show tcp
- show tcp brief
- show tcp statistics
- show tcp tcb

3.1.1 clear tcp

Syntax

To delete a TCP connection, run the following command:
clear tcp {**local** *host-name port* **remote** *host-name port* | **tcb** *address*}

Parameters

Parameters	Description
local host-name port	IP address and TCP port of the local host

remote host-name port	IP address and TCP port of the remote host
tcb address	Address of the transmission control block (TCB) for the to-be-deleted TCP connection TCB is an internal identifier of the TCP connection, which can be obtained through the show tcp brief command.

Command Mode

EXEC

Usage Guidelines

The clear tcp command is mainly used to delete the terminated TCP connection. The clear tcp command is mainly used to delete the terminated TCP connection. The TCP connection has no communication, so the system does not know that the TCP connection is already closed. In this case, the clear tcp command is used to close the invalid TCP connection. The clear tcp local host-name port remote host-name port command is used to close the TCP connection between the IP address or port of the local host and the IP address or port of the remote host. The clear tcp tcb address command is used to close the TCP connection identified by the designated TCB address.

Example

The following example shows that the TCP connection between 192.168.20.22:23 (local) and 192.168.20.120:4420 (remote). The show tcp brief command is used to display the information of the local and remote hosts of the current TCP connection.

```
switch#show tcp brief
TCB          Local Address        Foreign Address      State
0xE85AC8     192.168.20.22:23     192.168.20.120:4420  ESTABLISHED
0xEA38C8     192.168.20.22:23     192.168.20.125:1583  ESTABLISHED
switch#clear tcp local 192.168.20.22 23 remote 192.168.20.120 4420
switch#show tcp brief
TCB          Local Address        Foreign Address      State
0xEA38C8     192.168.20.22:23     192.168.20.125:1583  ESTABLISHED
```

The following example shows how to clear the TCP connection whose TCB address is 0xea38c8. The show tcp brief command displays the TCB address of the TCP connection.

```
switch#show tcp brief
TCB          Local Address        Foreign Address      State
0xEA38C8     192.168.20.22:23     192.168.20.125:1583  ESTABLISHED
switch#clear tcp tcb 0xea38c8
switch#show tcp brief
TCB          Local Address        Foreign Address      State
```

Related Command

show tcp
show tcp brief
show tcp tcb

3.1.2 clear tcp statistics

Syntax

To clear the statistics data about TCP, run the following command:
clear tcp statistics

Parameters

The command has no parameters or keywords.

Command Mode

EXEC

Example

The following example shows how to delete the TCP statistics information:
switch#clear tcp statistics

Related Command

show tcp statistics

3.1.3 debug arp

Syntax

To display the ARP interaction information, such as ARP request transmitting, ARP response receiving, ARP request receiving and ARP response transmitting, run debug arp. When the switch and host cannot communicate with each other, you can run the command to analyze the ARP interaction information. You can run no debug arp to stop displaying the ARP interaction information. To disable displaying the ARP interaction information, run this command.
debug arp [***packet | delete*** **]**
no debug arp

Parameters

Parameters	Description

packet	The debug information of ARP packet and entry
delete	The deleted debug information of ARP entry

Command Mode

EXEC

Example

switch#debug arp

switch#IP ARP: rcvd req src 192.168.20.116 00:90:27:a7:a9:c2, dst 192.168.20.111, vlan 10

IP ARP: req filtered src 192.168.20.139 00:90:27:d5:a9:1f, dst 192.168.20.82 00:

00:00:00:00:00, wrong cable, vlan 11

IP ARP: created an incomplete entry for IP address 192.168.20.77, vlan 10

IP ARP: sent req src 192.168.20.22 08:00:3e:33:33:8a, dst 192.168.20.77, vlan 10

IP ARP: rcvd reply src 192.168.20.77 00:30:80:d5:37:e0, dst 192.168.20.22, vlan 10

The first information line shows that the swtich receives an ARP request from Ethernet vlan 10. The ARP is sent from a host whose IP address is 192.168.20.116 and MAC address is 00:90:27:a7:a9:c2 and received by a host whose IP address is 192.168.20.111. The ARP request requires the MAC address of the destination host.

IP ARP: rcvd req src 192.168.20.116 00:90:27:a7:a9:c2, dst 192.168.20.111, vlan 10

The second information line shows that the switch receives an ARP address request with IP 192.168.20.139 from interface Etherner vlan 11. However, according to the interface configuration of the switch, the interface is not in the network claimed by the host. The reason may lie in the incorrect host configuration. If the switch creates an ARP cache according to the information, it cannot communicate with a host having the same address though the host connects an interface normally.

IP ARP: req filtered src 192.168.20.139 00:90:27:d5:a9:1f, dst 192.168.20.82 00:

00:00:00:00:00, wrong cable, vlan 11

The third line shows that, before the switch resolves the MAC address of host 192.168.20.77, an incomplete ARP item must be created in the ARP cache for the host; after the ARP response is received, the MAC address is entered. According to the configuration of the switch, the host connects interface Ethernet vlan 10.

IP ARP: created an incomplete entry for IP address 192.168.20.77, vlan 10

The fourth information shows that the switch transmits the ARP request from interface Ethernet vlan 10, the IP address of the switch is 192.168.20.22, the MAC address of the interface is 08:00:3e:33:33:8a and the IP address of the requested host is 192.168.20.77. The four information line has connection with the third information line.

IP ARP: sent req src 192.168.20.22 08:00:3e:33:33:8a, dst 192.168.20.77, vlan 10

The fifth information line shows the switch receives the ARP response which is transferred from host

192.168.20.77 to the switch's interface 192.168.20.22 on interface Ethernet 1/0, telling that the MAC address is 00:30:80:d5:37:e0. The fifth information line has connection with the third and fourth information lines.

IP ARP: rcvd reply src 192.168.20.77 00:30:80:d5:37:e0, dst 192.168.20.22, vlan 10

3.1.4 debug ip icmp

Syntax

To display the interaction information about ICMP, run the following command. To disable the debugging output, run no debug ip icmp.

debug ip icmp

no debug ip icmp

Parameters

The command has no parameters or keywords.

Command Mode

EXEC

Usage Guidelines

The command is used to display the received and transmitted ICMP packets, helping to resolve the end-to-end connection problem. To understand the detailed meaning of the debug ip icmp command, see RFC 792, "Internal Control Message Protocol".

Example

switch#debug ip icmp

switch#ICMP: sent pointer indicating to 192.168.20.124 (dst was 192.168.20.22), len 48

ICMP: rcvd echo from 192.168.20.125, len 40

ICMP: sent echo reply, src 192.168.20.22, dst 192.168.20.125, len 40

ICMP: sent dst (202.96.209.133) host unreachable to 192.168.20.124, len 36

ICMP: sent dst (192.168.20.22) protocol unreachable to 192.168.20.124, len 36

ICMP: rcvd host redirect from 192.168.20.77, for dst 22.0.0.3 use gw 192.168.20.26, len 36

ICMP: rcvd dst (22.0.0.3) host unreachable from 192.168.20.26, len 36

ICMP: sent host redirect to 192.168.20.124, for dst 22.0.0.5 use gw 192.168.20.77, len 36

ICMP: rcvd dst (2.2.2.2) host unreachable from 192.168.20.26, len 36

The first information line is explained as follows:

ICMP: sent pointer indicating to 192.168.20.124 (dst was 192.168.20.22), len 48

Domain	Description
ICMP	Displays the information about (ICMP)
Sent	Transmits the ICMP packets.

pointer indicating	Type of the ICMP packet, which shows the original IP packet is incorrect and specifies the incorrect domain. Other types of ICMP packet include: echo reply (echo reply) dst unreachable including: ---net unreachable(net unreachable) ---host unreachable（host unreachable） ---protocol unreachable（protocol unreachable） ---port unreachable（port unreachable） ---fragmentation needed and DF set（fragmentation needed and DF set） ---source route failed（source route failed） ---net unknown（net unknown） ---destination host unknown（destination host unknown） ---source host isolated(source host isolated) ---net prohibited（net prohibited） ---host prohibited（host prohibited） ---net tos unreachable（net tos unreachable） ---host tos unreachable（host tos unreachable） source quench（source quench） redirect(redirection), including: ---net redirect(net redirect) ---host redirect(host redirect) ---net tos redirect(redirection for the service type and the network) ---host tos redirect(redirection for the service type and the host) echo（echo request） router advertisement router solicitation time exceeded（timeout），including： ---ttl exceeded（ttltimeout） ---reassembly timeout（reassembly timeout） parameter problem（parameter problem），including： ---pointer indicating（point error parameter） ---option missed（option missed） ---bad length（bad length） timestamp（timestamp） timestamp reply（timestamp reply） information request（information request） information reply（information reply） mask request（mask request） mask reply（mask reply）

to 192.168.20.124	The destination address of the ICMP packet is 192.168.20.124, which is also the source address, of the original packet triggering the ICMP packet.
(dst was 192.168.20.22)	The destination address of the original packet leading to the ICMP packet is 192.168.20.22.
len 48	The length of the ICMP packet is 48bytes, the length of IP header excluded.

The second information line is explained as follows:

ICMP: rcvd echo from 192.168.20.125, len 40

Domain	Description
rcvd	Receives the ICMP packet.
echo	ICMPICMP packet type, Request response packet
from 192.168.20.125	The source address of the ICMP packet is192.168.20.125.

The third information line is explained as follows:

ICMP: sent echo reply, src 192.168.20.22, dst 192.168.20.125, len 40

Domain	Command
src 192.168.20.22	The source address of the ICMP packet is192.168.20.125.
dst 192.168.20.125	The destination address of the ICMP packet is 192.168.20.125.

Different types of ICMP packets have different formats when the ICMP packet is generated.

For example, the ICMP redirect packet adopts the following format:

ICMP: rcvd host redirect from 192.168.20.77, for dst 22.0.0.3 use gw 192.168.20.26, len 36

ICMP: sent host redirect to 192.168.20.124, for dst 22.0.0.5 use gw 192.168.20.77, len 36

The first information line shows that the redirect ICMP packet from host 192.168.20.77 is received and gateway 192.168.20.26 is recommended to forward the packet to destination host 22.0.0.3; the length of the ICMP packet is 36 bytes.

The second information line shows the redirect ICMP packet is sent to host 192.168.20.124. The redirect ICMP packet notifies the host of using gateway 192.168.20.77 to send packets to host 22.0.0.5. The length of the ICMP packet is 36 bytes.

For the DST unreachable ICMP packet, the following format is adopted for printing:

ICMP: sent dst (202.96.209.133) host unreachable to 192.168.20.124, len 36

ICMP: rcvd dst (2.2.2.2) host unreachable from 192.168.20.26, len 36

The first information line shows that, because the switch cannot route a certain IP packet, the source host 192.168.20.124 sends the unreachable ICMP packet to the destination host (202.96.209.133). The length of the ICMP packet is 36 bytes.

The second information line shows that the switch receives an ICMP packet from host 192.168.20.26, notifying that the destination host 2.2.2.2 cannot be reached. The length of the ICMP packet is 36 bytes.

3.1.5 debug ip packet

Syntax

To display the information about IP interaction, run debug ip raw. To disable displaying the IP interaction information, use the no form of this command.

debug ip packet [**detail**] *[***access-group** *ip-access-list-name*] [**interface** *type number*]

no debug ip packet

Parameters

Parameters	Description
detail	(optional) exports the protocol information encapsulated by the IP packet, such as the protocol number, number of the UDP port and the TCP port, and ICMP packet type.
ip-access-list-name	(optional) name of the IP ACL which is used to filter the output information Only the information about the IP packets that comply with the designated IP ACL can be exported.
interface	(optional) interface name which is used to filter the output information Only the information about the IP packets that comply with the designated port can be exported.

Command Mode

EXEC

Usage Guidelines

The command helps you to know the final destination of each received or locally-generated IP flows and to find the reason of the communication problem.

The following are potential cases:

- Forwarded
- Forwarded as the broadcast/multicast packet
- Failed addressing when the IP packet is forwarded
- Forwarding the redirect packet
- Rejected because of having the source route option
- Rejected because of illegal IP options
- Source route
- Locally-transmitted packets need fragmentation, while the DF bit is reset.
- Receiving the packets
- Receiving IP fragments
- Transmitting packets
- Transmitting the broadcast/multicast
- Failed addressing of locally-generated packets
- Locally-generated packets being fragmented

- Received packets being filtered
- Transmitted packets being filtered
- Encapsulation of the link layer failed (only for Ethernet)
- Unknown protocol

If you use the command, lots of output information will appear; you had better run the switch at a relatively free time, or the system's performance may be badly affected. Additionally, you had better filter the information output through the access list, enabling the system to display the information that interests users.

Command Mode

EXEC

Example

switch#debug ip packet

switch#IP: s=192.168.20.120 (vlan 10), d=19.0.0.9 (vlan 10), g=192.168.20.1, len=60, redirected

IP: s=192.168.20.22 (local), d=192.168.20.120 (vlan 10), g=192.168.20.120, len=56, sending

IP: s=192.168.20.120 (vlan 10), d=19.0.0.9 (vlan 10), g=192.168.20.1, len=60, forward

IP: s=192.168.20.81 (vlan 10), d=192.168.20.22 (vlan 10), len=56, rcvd

Domain	Description
IP	Means that the information is about the IP packet.
s=192.168.20.120 (vlan 10)	Source address of the IP packet and the name of the interface receiving the packet
d=19.0.0.9 (vlan 10)	Destination address of the IP packet and the name of the interface transmitting the packet (if the routing succeeds)
g=192.168.20.1	Destination address of the next hop of the IP packet, which may be the gateway address or the destination address
len	Length of the IP packet

redirected	Means the switch will send the ICMP redirected packet to the source host of the ICMP packet. The following are other cases: Forward—the packet is forwarded. forward directed broadcast---Packets are forwarded as the directed broadcast and packets will be transformed as the physical broadcast on the transmission interface unroutable---The addressing of the packet fails and and the packet will be dropped. source route---Source route rejected source route---Because the system does not support the source route, the packets with the IP source route are rejected. Bad options—the IP option is incorrect and the packet will be dropped. need frag but DF set---The local packet need be fragmented; however, the DF is reset. rcvd---the packet is received by the local host. rcvd fragment---The fragment of the packet is received. sending---The locally-generated packet is being sent. sending broad/multicast---The locally-generated broadcast/multicast packet is being sent. sending fragment---The locally-fragmented IP packet is being sent. denied by in acl---The packet is denied by the ACL of the receiver interface. denied by out acl---The packet is denied by the transmitter interface. unknown protocol---unknown protocol encapsulation failed---the protocol encapsulation fails in the Ethernet. When the to-be-transmitted packet is dropped on the Ethernet interface because of ARP resolution failure, the information appears.

The first information line shows that the switch has received an IP packet; its source address is 192.168.20.120 and destination address is 19.0.0.9; it is from the network segment connected by interface vlan 10; the transmitter interface determined by the routing table is interface vlan 10; the gateway's address is 192.168.20.1 and the length of the packet is 60 bytes. The gateway and the source host which transmits the IP packet are connected on the same network, that is, the network connected by interface vlan 10 of the switch. Hence, the switch transmits the ICMP redirect packet.

IP: s=192.168.20.120 (vlan 10), d=19.0.0.9 (vlan 10), g=192.168.20.1, len=60, redirected

The second information line describes the transmission of the ICMP redirect packet. The source address is the local address 192.168.20.22 and the destination address is the source address of the previous packet, that is, 192.168.20.120. The ICMP redirect packet is transmitted from interface vlan 10 to the destination directly, so the address of the gateway is the destination address 192.168.20.120. The length of the ICMP redirect packet is 56 bytes.

IP: s=192.168.20.22 (local), d=192.168.20.120 (vlan 10), g=192.168.20.120, len=56, sending

The third information line shows that the IP layer receives an IP packet. The source address of the packet is 192.168.20.120; the transmitter interface is interface vlan 10; the destination address of the

packet is 19.0.0.9. Through the routing table, the packet is found to forward to interfaceVLAN 10; the address of the gateway is 192.168.20.77 and the length of the packet is 60 bytes. This information shows the packet displayed when forwarding the first information after the system sends ICMP redirection packets.

IP: s=192.168.20.120 (vlan 10), d=19.0.0.9 (vlan 10), g=192.168.20.77, len=60, forward

The fourth information line shows that the IP layer receives an IP packet. The source address is 192.168.20.81 and the receiver interface isVLAN 10; the destination address is 192.168.20.22, which is an IP address configured on interfaceVLAN 10of the switch; the length of the packet is 56 bytes.

IP: s=192.168.20.81 (vlan 10), d=192.168.20.22 (vlan 10), len=56, rcvd

The output of the debug ip packet detail command is described in the following. Only newly-added parts are described.

switch#debug ip packet detail

switch#IP: s=192.168.12.8 (vlan 10), d=255.255.255.255 (vlan 10), len=328, rcvd, UDP: src=68, dst=67

IP: s=192.168.20.26 (vlan 10), d=224.0.0.5 (vlan 10), len=68, rcvd, proto=89

IP: s=192.168.20.125 (vlan 10), d=192.168.20.22 (vlan 10), len=84, rcvd, ICMP: type=0, code = 0

IP: s=192.168.20.22 (local), d=192.168.20.124 (vlan 10), g=192.168.20.124, len=40, sending, TCP: src=1024, dst=23, seq=75098622, ack=161000466, win=17520, ACK

Domain	Description
UDP	Protocol name, such as UDP, ICMP or TCP. Other protocols are presented with the protocol number.
type, code	Type and code of the ICMP packet
src, dst	Source port and destination port of the UDP/TCP packet
seq	Sequence number of the TCP packet
ack	Acknowledge number of the TCP packet
win	Windows value of the TCP packet
ACK	ACK in the control bit of the TCP packet is reset, indicating that the acknowledge number is valid. Other control bits include SYN, URG, FIN, PSH and RST.

The first information line shows that the UDP packet is received. The source port is 68 and the destination port is 67.

IP: s=192.168.12.8 (vlan 10), d=255.255.255.255 (vlan 10), len=328, rcvd, UDP: src=68, dst=67

The second information line shows that the protocol number of the received packet is 89.

IP: s=192.168.20.26 (vlan 10), d=224.0.0.5 (vlan 10), len=68, rcvd, proto=89

The third information line shows that the ICMP packet is received. Both the packet type and the code are 0.

IP: s=192.168.20.125 (vlan 10), d=192.168.20.22 (vlan 10), len=84, rcvd, ICMP: type=0, code = 0

The fourth information line shows that the TCP packet is transmitted. The source port is 1024, the destination port is 23, the sequence number is 75098622, the acknowledge number is 161000466,

the size of the receiver window is 17520 and the ACK bit is reset. For the meanings of these domains, see RFC 793— TRANSMISSION CONTROL PROTOCOL.

IP: s=192.168.20.22 (local), d=192.168.20.124 (vlan 10), g=192.168.20.124, len=40, sending, TCP: src=1024, dst=23, seq=75098622, ack=161000466, win=17520, ACK

The following describes how to use the ACL. For example, to display the information about the packet whose source address is 192.168.20.125, you need to define the abc ACL and then allow the IP packets whose source address is 192.168.20.125. At last, you can use the ACL in the debug ip packet command.

switch#config

switch_config#ip access-list standard abc

switch_config_std_nacl#permit 192.168.20.125

switch_config_std_nacl#exit

switch_config#exit

switch#debug ip packet access-group abc

switch#IP: s=192.168.20.125 (vlan 101), d=192.168.20.22 (vlan 101), len=48, rcvd

In the previous commands, the standard ACL is used. However, the expanded ACL can also be used.

Related Command

debug ip tcp packet

3.1.6 debug ip raw

Syntax

To display the information about IP interaction, run debug ip raw. To disable displaying information about IP interaction, run no debug ip raw.

debug ip raw [**detail**] [*access*-**group** ***access-list-group***] [**interface** ***type number***]

no debug ip raw

Parameters

Parameters	Description
detail	(optional) exports the protocol information encapsulated by the IP packet, such as the protocol number, number of the UDP port and the TCP port, and ICMP packet type.
access-list-group	(optional) name of the IP ACL which is used to filter the output information Only the information about the IP packets that comply with the designated IP ACL can be exported.
interface	(optional) interface name which is used to filter the output information Only the information about the IP packets that comply with the designated port can be exported.

Command Mode

EXEC

Usage Guidelines

The command helps you to know the final destination of each received or locally-generated IP flows and to find the reason of the communication problem.
The following are potential cases:

- Forwarded
- Forwarded as the broadcast/multicast packet
- Failed addressing when the IP packet is forwarded
- Forwarding the redirect packet
- Rejected because of having the source route option
- Rejected because of illegal IP options
- Source route
- Locally-transmitted packets need fragmentation, while the DF bit is reset.
- Receiving the packets
- Receiving IP fragments
- Transmitting packets
- Transmitting the broadcast/multicast
- Failed addressing of locally-generated packets
- Locally-generated packets being fragmented
- Received packets being filtered
- Transmitted packets being filtered
- Encapsulation of the link layer failed (only for Ethernet)
- Unknown protocol

If you use the command, lots of output information will appear; you had better run the switch at a relatively free time, or the system's performance may be badly affected. Additionally, you had better filter the information output through the access list, enabling the system to display the information that interests users.

Example

It is the same with debug ip packet, so it is omitted here.

Related Command

debug ip tcp packet

3.1.7 debug ip tcp packet

Syntax

To display the information about receiving and transmitting the TCP packet, run debug ip tcp packet. To disable displaying relative information, run no debug ip tcp packet.

debug ip tcp packet
no debug ip tcp packet

Parameters

The command has no parameters or keywords.

Command Mode

EXEC

Example

```
switch#debug ip tcp packet
switch#tcp: O ESTABLISHED 192.168.20.22:23 192.168.20.125:3828 seq 50659460
        DATA 1 ACK 3130379810 PSH WIN 4380
tcp: I ESTABLISHED 192.168.20.22:23 192.168.20.125:3828 seq 3130379810
        DATA 2 ACK 50659460 PSH WIN 16372
tcp: O ESTABLISHED 192.168.20.22:23 192.168.20.125:3828 seq 50659461
        DATA 50 ACK 3130379812 PSH WIN 4380
tcp: O FIN_WAIT_1 192.168.20.22:23 192.168.20.125:3828 seq 50659511
        ACK 3130379812 FIN WIN 4380
tcp: I FIN_WAIT_1 192.168.20.22:23 192.168.20.125:3828 seq 3130379812
        ACK 50659511 WIN 16321
tcp: I FIN_WAIT_1 192.168.20.22:23 192.168.20.125:3828 seq 3130379812
        ACK 50659512 WIN 16321
tcp: I FIN_WAIT_2 192.168.20.22:23 192.168.20.125:3828 seq 3130379812
        ACK 50659512 FIN WIN 16321
tcp: O TIME_WAIT 192.168.20.22:23 192.168.20.125:3828 seq 50659512
        ACK 3130379813 WIN 4380
tcp: I LISTEN 0.0.0.0:23 0.0.0.0:0 seq 3813109318
        DATA 2 ACK 8057944 PSH WIN 17440
```

tcp: O LISTEN 0.0.0.0:23 0.0.0.0:0 seq 8057944

RST

Domain	Description
tcp:	Information about the TCP packets
O	Transmits the TCP packets.
ESTABLISHED	TCP Current state of the TCP connection For the description of the TCP connection's state, see the description of the debug ip tcp transactions command.
192.168.20.22:23	The source address of the packet is 192.168.20.22 and the source port is 23.
192.168.20.125:3828	The destination address of the packetis 192.168.20.125 and the destination port is3828.
seq 50659460	The sequence number of the packet is50659460.
DATA 1	Means that the packet containsonly one effective byte.
ACK 3130379810	The acknowledgment number of the packet is 3130379810.
PSH	PSH is reset in the controlbit of the packet. Other control bytes include ACK,FIN,SYN,URG and RST.
WIN 4380	Window domain of the packet used to notify the peer end to receive the cache size, which is 4380 bytes currently4380bytes
I	Receives the TCP packet.

If a domain of the previous domains does not appear, the domain has no effective value in the TCP packet.

Related Command

debug ip tcp transactions

3.1.8 debug ip tcp transactions

Syntax

To display the important interaction information about TCP, such as the state change of the TCP connection, run debug ip tcp transactions. To disable displaying relative information, run no debug ip tcp transactions.

debug ip tcp transactions

no debug ip tcp transactions

Parameters

The command has no parameters or keywords.

Command Mode

EXEC

Example

switch#debug ip tcp transactions

switch#TCP: rcvd connection attempt to port 23

TCP: TCB 0xE88AC8 created

TCP: state was LISTEN -> SYN_RCVD [23 -> 192.168.20.125:3828]

TCP: sending SYN, seq 50658312, ack 3130379657 [23 -> 192.168.20.125:3828]

TCP: state was SYN_RCVD -> ESTABLISHED [23 -> 192.168.20.125:3828]

TCP: connection closed by user, state was LISTEN [23 -> 0.0.0.0:0]

TCP: state was TIME_WAIT -> CLOSED [23 -> 192.168.20.125:3827]

TCP: TCB 0xE923C8 deleted

TCP: TCB 0xE7DBC8 created

TCP: connection to 192.168.20.124:513 from 192.168.20.22:1022, state was CLOSED to SYN_SENT

TCP: sending SYN, seq 52188680, ack 0 [1022 -> 192.168.20.124:513]

TCP: state was SYN_SENT -> ESTABLISHED [1022 -> 192.168.20.124:513]

TCP: rcvd FIN, state was ESTABLISHED -> CLOSE_WAIT [1022 -> 192.168.20.124:513]

TCP: connection closed by user, state was CLOSE_WAIT [1022 -> 192.168.20.124:513]

TCP: sending FIN [1022 -> 192.168.20.124:513]

TCP: connection closed by user, state was LAST_ACK [1022 -> 192.168.20.124:513]

TCP: state was LAST_ACK -> CLOSED [1022 -> 192.168.20.124:513]

TCP: TCB 0xE7DBC8 deleted

Domain	Description
TCP:	Displays the TCPinteraction information.
rcvd connection attempt to port 23	Receives the connection request from the peer port23（that is, the TELNET port.
TCB 0xE88AC8 created	Generates a new control block for the TCP connection, which is identified as 0xE88AC8.

state was LISTEN -> SYN_RCVD	Means that the TCP state machine changes from LISTEN to SYN_RCVD. The states of the TCP include: LISTEN—waiting for the TCP connection request from any remote host SYN_SENT—Sending out the connection request to trigger the TCP connection negotiation and then waiting for the peer's response SYN_RCVD—receiving the connection request from the peer, sending out the acknowledgment response and also sending out its connection request, and waiting for the connection request acknowledgment from the peer ESTABLISHED---means that the connection is created; the connection is in the data transmission phase; the data of the upper-layer application can be received and transmitted. FIN_WAIT_1—Means that the connection termination request has been transmitted and the response and connection termination request from the peer are being waited. FIN_WAIT_2—Means that the connection termination request has been transmitted and the response from the peer has been received, while the connection termination request from the peer is being waited. CLOSE_WAIT—Means the connection termination request of the peer is received and the local response has been sent out, and now the local user is being waited to close the connection. Once the user requires closing the connection, the system will send the connection termination request. CLOSING—Means the connection termination request has been sent to the peer and the peer's connection termination request is also received and the corresponding response is also sent out, and now is waiting for the peer to acknowledge the local connection termination request. LAST_ACK—Means that the connection termination request from the peer is received and acknowledged, and now the connection termination request is transmitted and the response is waited. TIME_WAIT—Means that a sufficient time is needed to ensure that the peer has already received the local acknowledgement of the peer's connection termination request and the connection packet still being transmitted in the network is waited to be sent to the destination or be dropped. CLOSED—Means that there is no connection or the connection has been completed shut down. For more detailed information, see RFC 793, TRANSMISSION CONTROL PROTOCOL.
[23 -> 192.168.20.125:3828]	The content in the bracket is explained as follows: The first domain (23) stands for the local TCP port. The second domain (192.168.20.125) stands for the remote IP address. The third domain(3828） stand for the remote TCP port.
sending SYN	Transmits a connection request out (the SYN of the control bit in the TCP header is reset). Other TCP control bits include SYN, ACK, FIN, PSH, RST and URG.
seq 50658312	The sequence number of the transmitted packet is 50658312.
ack 3130379657	The acknowledgement number of the transmitted packet is 3130379657.

rcvd FIN	Means that the connection termination request is received (FINin the control bit of the TCP header is reset).
connection closed by user	Means that the upper-layer application requires disabling the TCP connection.
connection timed out	Means that the connection is closed because it times out.

Related Command

debug ip tcp packet

3.1.9 debug ip udp

Syntax

To display the interaction information about UDP, run the following command. To stop displaying the information about UDP interaction, run no debug ip udp.

debug ip udp
no debug ip udp

Parameters

The command has no parameters or keywords.

Command Mode

EXEC

Example

switch#debug ip udp

switch#UDP: rcvd src 192.168.20.99(520), dst 192.168.20.255(520), len = 32

UDP: sent src 192.168.20.22(20001), dst 192.168.20.43(1001), len = 1008

Domain	Description
UDP:	Means that the information is about the UDP packet.
rcvd	Receiving the packets
sent	Means that the packet is transmitted.
src	Stands for the source IP address and UDP port of the UDP packet.
dst	Stands for the destination IP address and UDP port of the UDP packet.
len	Stands for the length of UDP packet.

The first information shows that the UDP packet is received. Its source address is 192.168.20.99 and its source port is port 520; its destination address is 192.168.20.255 and its destination port is port 520; the length of the packet is 32 bytes.

The second information shows that the UDP packet is transmitted. Its source address is

192.168.20.22 and its source port is port 20001; its destination address is 192.168.20.43 and its destination port is port 1001; the length of the packet is 1008 bytes.

3.1.10 ip mask-reply

Syntax

To enable the switch to answer the request of the IP mask on the designated interface, run ip mask-reply. To disable this function, run no ip mask-reply.

ip mask-reply
no ip mask-reply
default ip mask-reply

Parameters

The command has no parameters or keywords.

Default Value

The IP mask request is not answered.

Command Mode

Interface configuration mode

Example

```
interface vlan 11
ip mask-reply
```

3.1.11 ip mtu

Syntax

To set the MTU of the IP packet transmitted from an interface, run ip mtu bytes. To reuse the default value of MTU, run no ip mtu.

ip mtu *bytes*
no ip mtu

Parameters

Parameters	Description
bytes	Maximum IP transmission length which is counted with bytes

Default Value

The physical media of the interfaces are different, while the MTU on the interfaces are same. Sixty-eight bytes is the minimum MTU.

Command Mode

Interface configuration mode

Usage Guidelines

If the length of the IP message exceeds IP MTU configured on the interface, the switch fragments the message. All devices connecting on the same physical media need be configured the same MTU. The MTU affects the IP MTU. If the value of IP MTU is the same as that of the MTU, the value of IP MTU automatically changes to the new value of the MTU when the MTU value changes. The change of the IP MTU does not affectthe MTU.
The minimum value of IP MTU is 68 bytes and the maximum value of IP MTU cannot exceed the MTU value configured on the interface.

Example

The following example shows that IP MTU on interface vlan 10 is set to 200:

```
interface vlan 10
ip mtu 200
```

Related Command

mtuip source-route

3.1.12 ip source-route

Syntax

To enable the switch to handle the IP packet with the source IP route option, run ip source-route. To enable the switch to drop the IP packet with the source IP route option, run no ip source-route.

ip source-route
no ip source-route

Parameters

None

Default Value

The IP packet with the source IP route option is handled.

Command Mode

Global configuration mode

Example

The following example shows how to enable the switch to handle the IP packet with the source IP route option.

ip source-route

Related Command

ping

3.1.13 ip tcp synwait-time

Syntax

To set the timeout time for the switch to wait for the successful TCP connection, run ip tcp synwait-time. To resume the default timeout time, run no ip tcp synwait-time.

ip tcp synwait-time *seconds*

no ip tcp synwait-time

Parameters

Parameters	Description
seconds	Time for the TCP connection, whose unit is second. The valid vale ranges between 5 and 300 seconds. The default value is 75.

Default Value

75 seconds

Command Mode

Global configuration mode

Usage Guidelines

When the switch triggers the TCP connection and if the TCP connection is not established in the designated wait time, the switch views that the connection fails and then sends the result to the upper-layer program. You can set the wait time for creation of the TCP connection. The default value of the wait time is 75 seconds. The option has no relation with the TCP connection packet which is forwarded through the switch, but has relation with the TCP connection of the switch itself.

Example

The following example shows how to set the wait time of creating TCP connection to 30 seconds:

switch_config#ip tcp synwait-time 30

3.1.14 ip tcp window-size

Syntax

To resume the default size of the TCP window, run no ip tcp window-size.

ip tcp window-size *bytes*

no ip tcp window-size

Parameters

Parameters	Description
bytes	Size of the window The maximum window size is 65535 bytes. The default window size is 2000 bytes.

Default Value

2000 bytes

Command Mode

Global configuration mode

Usage Guidelines

Do not change the window size at will unless you have a definite purpose.

Example

The following example shows how to set the size of the TCP window to 6000 bytes.

switch_config#ip tcp window-size 6000

3.1.15 ip unreachables

Syntax

To enable the switch to transmit the ICMP unreachable packet, run ip unreachable. To enable the switch to stop transmitting this packet, run no ip unreachable.

ip unreachables

no ip unreachables

Parameters

The command has no parameters or keywords.

Default Value

ICMP unreachable packets are sent by default.

Command Mode

Interface configuration mode

Usage Guidelines

When the switch forwards the IP packet, the packet may be dropped because there is no relative route in the routing table. In this case, the switch can send the ICMP unreachable packet to the source host, notifying the source host and enabling it to detect the host timely and correct the fault rapidly.

Example

The following example shows how to enable the ICMP unreachable packet to be transmitted on interface vlan 10:

interface vlan 10

ip unreachables

3.1.16 show ip sockets

Syntax

To display the socket information, run this command.
show ip sockets *[socketid]*

Parameters

Parameters	Description
socketid	Displays some socket information.

Command Mode

EXEC

Example

switch#show ip sockets

Proto	Local	Port	Remote	Port	In	Out
17	0.0.0.0	0	0.0.0.0	0	161	0
6	0.0.0.0	0	0.0.0.0	0	513	0
17	0.0.0.0	0	0.0.0.0	0	1698	0
17	0.0.0.0	0	0.0.0.0	0	69	0
6	0.0.0.0	0	0.0.0.0	0	23	0
17	0.0.0.0	0	0.0.0.0	0	137	122590

Domain	Description
Proto（Protocol）	IP Protocol ID 17 is UDP and 6 is TCP
Remote (Remote)	Remote address
Port (Port)	Remote port
Local(local)	Local address
Port (Port)	Local port
In(receive)	Total number of the received bytes
Out(send)	Total number of the received bytes

3.1.17 show ip traffic

Syntax

To display the flow statistics information, run the following command:
show ip traffic

Parameters

The command has no parameters or keywords.

Command Mode

EXEC

Example

switch#show ip traffic

IP statistics:

Rcvd: 0 total, 0 local destination, 0 delivered

0 format errors, 0 checksum errors, 0 bad ttl count

0 bad destination address, 0 unknown protocol, 0 discarded

0 filtered , 0 bad options, 0 with options

Opts: 0 loose source route, 0 record route, 0 strict source route

0 timestamp, 0 router alert, 0 others

Frags: 0 fragments, 0 reassembled, 0 dropped

0 fragmented, 0 fragments, 0 couldn't fragment

Bcast: 0 received, 0 sent

Mcast: 0 received, 0 sent

Sent: 230 generated, 0 forwarded

0 filtered, 0 no route, 0 discarded

ICMP statistics:

Rcvd: 0 total, 0 format errors, 0 checksum errors

0 redirect, 0 unreachable, 0 source quench

0 echos, 0 echo replies, 0 mask requests, 0 mask replies

0 parameter problem, 0 timestamps, 0 timestamp replies

0 time exceeded, 0 router solicitations, 0 router advertisements

Sent: 0 total, 0 errors

0 redirects, 0 unreachable, 0 source quench

0 echos, 0 echo replies, 0 mask requests, 0 mask replies

0 parameter problem, 0 timestamps, 0 timestamp replies

0 time exceeded, 0 router solicitations, 0 router advertisements

UDP statistics:

Rcvd: 28 total, 0 checksum errors, 22 no port, 0 full sock

Sent: 0 total

TCP statistics:

Rcvd: 0 total, 0 checksum errors, 0 no port

Sent: 3 total

IGMP statistics:

Rcvd: 0 total, 0 format errors, 0 checksum errors

0 host queries, 0 host reports

Sent: 0 host reports

ARP statistics:

Rcvd: 8 total, 7 requests, 1 replies, 0 reverse, 0 other

Sent: 5 total, 5 requests, 0 replies (0 proxy), 0 reverse

Domain	Description
format errors(format errors)	Error of the packet's format, such as incorrect IP header length
bad hop count(TTLerror)	If the routing switch finds that the TTL value of the packet decreases to zero when it forwards the packet, the packet will be dropped.
no route(no route)	Means that the switch has no corresponding route.

3.1.18 show tcp

Syntax

To display all status information of TCP connection, run the following command.
show tcp

Parameters

The command has no parameters or keywords.

Command Mode

EXEC

Example

switch#show tcp

TCB 0xE9ADC8

Connection state is ESTABLISHED, unread input bytes: 934

Local host: 192.168.20.22, Local port: 1023

Foreign host: 192.168.20.124, Foreign port: 513

Enqueued bytes for transmit: 0, input: 934 mis-ordered: 0 (0 packets)

Timer	Starts	Wakeups	Next(ms)
Retrans	33	1	0
TimeWait	0	0	0
SendWnd	0	0	0
KeepAlive	102	0	7199500

iss: 29139463 snduna: 29139525 sndnxt: 29139525 sndwnd: 17520

irs: 709124039 rcvnxt: 709205436 rcvwnd: 4380

SRTT: 15 ms, RXT: 2500 ms, RTV: 687 ms

minRXT: 1000 ms, maxRXT: 64000 ms, ACK hold: 200 ms

Datagrams (max data segment is 1460 bytes):

Rcvd: 102 (out of order: 0), with data: 92, total data bytes: 81396

Sent: 104 (retransmit: 0), with data: 31, total data bytes: 61

Domain	Description
TCB 0xE77FC8	Internal identifier of the control block for the TCP connection

Connection state is ESTABLISHED	Current state of the TCP connection The TCP connection may be in one of the following states: LISTEN---Means the TCP connection request from any remote host is being waited. SYN_SENT---Means that the response from the peer is being waited after the connection request is transmitted to the peer. SYN_RCVD—receiving the connection request from the peer, sending out the acknowledgment response and also sending out its connection request, and waiting for the connection request acknowledgment from the peer ESTABLISHED---means that the connection is created; the connection is in the data transmission phase; the data of the upper-layer application can be received and transmitted. FIN_WAIT_1—Means that the connection termination request has been transmitted and the response and connection termination request from the peer are being waited. FIN_WAIT_2—Means that the connection termination request has been transmitted and the response from the peer has been received, while the connection termination request from the peer is being waited. CLOSE_WAIT—Means the connection termination request of the peer is received and the local response has been sent out, and now the local user is being waited to close the connection. Once the user requires closing the connection, the system will send the connection termination request. CLOSING—Means the connection termination request has been sent to the peer and the peer's connection termination request is also received and the corresponding response is also sent out, and now is waiting for the peer to acknowledge the local connection termination request. LAST_ACK—Means that the connection termination request from the peer is received and acknowledged, and now the connection termination request is transmitted and the response is waited. TIME_WAIT—Means that a sufficient time is needed to ensure that the peer has already received the local acknowledgement of the peer's connection termination request and the connection packet still being transmitted in the network is waited to be sent to the destination or be dropped. CLOSED—Means that there is no connection or the connection has been completed shut down. For more detailed information, see RFC 793, TRANSMISSION CONTROL PROTOCOL.
unread input bytes:	Data that is submitted to but not yet received by the upper-layer application after the lower-layer TCP handles
Local host:	Local IP address
Local port:	Local TCP port
Foreign host:	Remote IP address
Foreign port:	Remote TCP port.

Enqueued bytes for transmit:	Bytes in the transmission queue, including the transmitted but unacknowledged data bytes and not-yet-transmitted data bytes
input:	Data in the receiver queue which is waiting for being received by the upper-layer application after sorting
mis-ordered:	Number of bytes and number of packets in the mis-ordered queue. These data can enter the receiver queue in order and be received by the upper-layer application after other data is received. For example, if packets 1, 2, 4, 5 and 6 are received, packets 1 and 2 can enter the receiver queue, while packets 4, 5 and 6 have to enter the mis-ordered queue to wait for the arrival of packet 3.

The information about the currently-displayed timer will then be displayed, including start-up times, timeout times and next timeout time (0 means the timer doesn't work currently). Each connection has its independent timers. The timeout times of the timer are generally less than the start-up times of the timer because the timer may be reset when it is running. For example, if the system receives the peer's acknowledgment of all transmitted data when the re-sending timer runs, the re-sending timer will stop running.

Timer	Starts	Wakeups	Next(ms)
Retrans	33	1	0
TimeWait	0	0	0
SendWnd	0	0	0
KeepAlive	102	0	7199500

Domain	Description
Timer	Name of the timer
Starts	Start-up times of the timer
Wakeups	Timeout times of the timer
Next(ms)	Time before next timeout occurs (unit: millisecond)0 means that the timer is not running.
Retrans	Retransmission timer which is used to retransmit the data. The timer is restarted after the data is transmitted. If the data is not acknowledged by the peer during the timeout time, the data will be resent.
TimeWait	Time-wait timer which is used to ensure that the peer receives the acknowledgement of the connection termination request.
SendWnd	Timer of the transmission timer, used to ensure that the receiver window resumes the normal size after the TCP acknowledgment is lost.
KeepAlive	KeepAlive timer used to ensure that the communication link is normal and the peer is still in the connection state. It will trigger the transmission of the test packet to detect the state of the communication link and the peer's state.

The sequence number of the TCP connection will then be displayed. The reliable and ordered data transmission is guaranteed through the sequence number. The local/remote host conducts flow control and transmission acknowledgment through the sequence number.

iss: 29139463 snduna: 29139525 sndnxt: 29139525 sndwnd: 17520

irs: 709124039 rcvnxt: 709205436 rcvwnd: 4380

Domain	Description
iss:	Initial transmission sequence number
snduna:	Transmission sequence number of the first byte in the data which has been transmitted but the peer's acknowledgment is not received
sndnxt:	Transmission sequence number of the first byte in the data which will be transmitted next time
sndwnd:	Size of the TCP window of the remote host.
irs:	Initial reception sequence number, that is, initial transmission sequence number of the remote host
rcvnxt:	Recently-acknowledged acceptation sequence number
rcvwnd:	Size of the TCP window of the local host

The transmission time recorded by the local host is then displayed. The system can adapt to different networks according to the data.

SRTT: 15 ms, RXT: 2500 ms, RTV: 687 ms

minRXT: 1000 ms, maxRXT: 64000 ms, ACK hold: 200 ms

Domain	Description
SRTT:	Round-trip time after smooth handle
RXT:	Retransmission timeout time
RTV:	Change value of the round-trip time
MinRXT:	Allowable minimum retransmission timeout
MaxRXT:	Allowable maximum retransmission timeout
ACK hold:	Maximum latency time for delaying the acknowledgment and enabling it to be transmitted together with the data

Datagrams (max data segment is 1460 bytes):

Rcvd: 102 (out of order: 0), with data: 92, total data bytes: 81396

Sent: 104 (retransmit: 0), with data: 31, total data bytes: 61

Domain	Description
max data segment is	Maximum data-segment length allowed by a connection
Rcvd:	Number of packets received by the local host through the connection and the number of mis-ordered packets
with data:	Number of packets which contains valid data
total data bytes:	Total data bytes contained in the packet
Sent	Total number of packets transmitted by the local host during the connection and the number of resent packets
with data:	Number of packets which contains valid data
total data bytes:	Total data bytes contained in the packet

Related Command

show tcp brief
show tcp tcb

3.1.19 show tcp brief

Syntax

To display the brief information about the TCP connection, run the following command:
show tcp brief [**all**]

Parameters

Parameters	Description
all	(optional) Displays all ports. If the keyword is not entered, the system will not display the port in listening mode.

Command Mode

EXEC

Example

```
switch#show tcp brief
TCB             Local Address               Foreign Address             State
0xE9ADC8        192.168.20.22:1023          192.168.20.124:513          ESTABLISHED
0xEA34C8        192.168.20.22:23            192.168.20.125:1472         ESTABLISHED
```

Domain	Description
TCB	TCP Internal identifier of the TCP connection
Local Address	Local address and local TCP port
Foreign Address	IP address and TCP port of the remote host.
State	State of the connection For details, see the show tcp command.

Related Command

show tcp
show tcp tcb

3.1.20 show tcp statistics

Syntax

To display the statistics data about TCP, run the following command.
show tcp statistics

Parameters

The command has no parameters or keywords.

Command Mode

EXEC

Example

```
switch#show tcp statistics
Rcvd: 148 Total, 0 no port
0 checksum error, 0 bad offset, 0 too short
131 packets (6974 bytes) in sequence
0 dup packets (0 bytes)
0 partially dup packets (0 bytes)
0 out-of-order packets (0 bytes)
0 packets (0 bytes) with data after window
0 packets after close
0 window probe packets, 0 window update packets
0 dup ack packets, 0 ack packets with unsend data
127 ack packets (247 bytes)
Sent: 239 Total, 0 urgent packets
6 control packets
123 data packets (245 bytes)
0 data packets (0 bytes) retransmitted
110 ack only packets (101 delayed)
0 window probe packets, 0 window update packets
4 Connections initiated, 0 connections accepted, 2 connections established
3 Connections closed (including 0 dropped, 1 embryonic dropped)
5 Total rxmt timeout, 0 connections dropped in rxmt timeout
```

1 Keepalive timeout, 0 keepalive probe, 1 Connections dropped in keepalive

Domain	Description
Rcvd:	Statistics data of the packets received by the switch
Total	Total number of the received packets
no port	Number of received packets which have no destination ports
checksum error	Number of received packets which have checksum error
bad offset	Number of received packets which have offset error
too short	Number of received packets whose length is less than the valid effective length
packets in sequence	Number of packets received in order
dup packets	Number of received duplicate packets
partially dup packets	Number of some duplicate packets received
out-of-order packets	Number of packets received out of order
packets with data after window	Number of received packets whose data exceeds the received window of the switch
packets after close	Number of packets received after the connection is closed
window probe packets	Number of received packets about window detection
window update packets	Number of received packets about window update
dup ack packets	Number of packets which are re-acknowledged after received
ack packets with unsent data	Number of packets which are received but not sent
ack packets	Number of acknowledgement packets
Sent	Statistics data of the packets transmitted by the switch
Total	Total number of the transmitted packets
urgent packets	Number of transmitted urgent packets
control packets	Total number of control packets (SYN, FIN or RST) which have been transmitted
data packets	Number of transmitted urgent packets
data packets retransmitted	Number of resent data packets
ack only packets	Number of transmitted acknowledgment packets
window probe packets	Number of transmitted packets about window detection
window update packets	Number of transmitted packets about window update
Connections initiated	Number of locally-initiated connections
connections accepted	Number of locally-accepted connections
connections established	Number of locally-established connections
Connections closed	Number of locally-closed connections
Total rxmt timeout	Total number of re-transmission timeouts
Connections dropped in rxmit timeout	Number of disconnected connections because of re-transmission timeout

Keepalive timeout	Number of keepalive timeouts
keepalive probe	Number of transmitted packets about keepalive detection
Connections dropped in keepalive	Number of connections which are disconnected because of Keepalive

Related Command

clear tcp statistics

3.1.21 show tcp tcb

Syntax

To display the state of a TCP connection, run the following command:
show tcp tcb address

Parameters

Parameters	Description
address	Address of the transmission control block (TCB) for the to-be-displayed TCP connection. TCB is an internal identifier of the TCP connection, which can be obtained through the show tcp brief command.

Command Mode

EXEC

Example

The following information is displayed after the show tcp command is run:

switch_config#show tcp tcb 0xea38c8

TCB 0xEA38C8

Connection state is ESTABLISHED, unread input bytes: 0

Local host: 192.168.20.22, Local port: 23

Foreign host: 192.168.20.125, Foreign port: 1583

Enqueued bytes for transmit: 0, input: 0 mis-ordered: 0 (0 packets)

Timer	Starts	Wakeups	Next(ms)
Retrans	4	0	0
TimeWait	0	0	0

SendWnd 0 0 0

KeepAlive +5 0 6633000

iss: 10431492 snduna: 10431573 sndnxt: 10431573 sndwnd: 17440

irs: 915717885 rcvnxt: 915717889 rcvwnd: 4380

SRTT: 2812 ms, RXT: 18500 ms, RTV: 4000 ms

minRXT: 1000 ms, maxRXT: 64000 ms, ACK hold: 200 ms

Datagrams (max data segment is 1460 bytes):

Rcvd: 5 (out of order: 0), with data: 1, total data bytes: 3

Sent: 4 (retransmit: 0), with data: 3, total data bytes: 80

Related Command

show tcp
show tcp brief

3.2 ACL Configuration Commands

ACL configuration commands include:

- deny
- ip access-group
- ip access-list
- permit
- show ip access-list

3.2.1 deny

Syntax

To configure the deny reglations in IP ACL configuration mode, run deny source [source-mask] or deny protocol source source-mask destination destination-mask [tos tos]. To remove a deny regulation from an IP ACL, run no deny source [source-mask] or no deny protocol source source-mask destination destination-mask [tos tos].

deny *source* [*source-mask*] **[log] [location**]

no deny *source* [*source-mask*] [**log**]

deny protocol source source-mask destination destination-mask [[**precedence** precedence] [**tos** tos] **[log] [offset-zero] [totallen] [time-range] [location] [ttl] [donotfragment-set]**

[donotfragment-notset] [is-fragment] [not-fragment] [offset-not-zero] [log]]

no deny protocol source source-mask destination destination-mask [[**precedence** precedence] [**tos** tos] [**log] [offset-zero] [totallen] [time-range] [location] [ttl] [donotfragment-set] [donotfragment-notset] [is-fragment] [not-fragment] [offset-not-zero] [log**]]

For the Internet Control Message Protocol (ICMP), use the following command syntax.

deny icmp source source-mask destination destination-mask [icmp-type] [**precedence** precedence] [**tos** tos] [log]

For the Internet Group Management Protocol (IGMP), run the following command syntax.

deny igmp source source-mask destination destination-mask [igmp-type] [**precedence** precedence] [**tos** tos] [log]

For the Transmission Control Protocol (TCP), use the following command syntax.

deny tcp source source-mask [operator port] destination destination-mask [operator port] [**established**] [**precedence** precedence] [**tos** tos] [log]

For the User Datagram Protocol (UDP), use the following command syntax.

deny udp source source-mask [operator port] destination destination-mask [operator port] [**precedence** precedence] [**tos** tos] [log]

Parameters

Parameters	Description
protocol	Stands for the protocol name or IP protocol number. It can be icmp, igmp, igrp, ip, ospf, tcp or udp, or it can be an integer from 0 to 255 which stands for the IP protocol. To match up any Internet protocol, including ICMP, TCP and UDP, you can use the ip keyword. Some protocols allow further limitations as described below.
source	Stands for a source network or host number. There are two methods to designate the source: 32-bit binary number or a decimal number separated by four points. The keyword any is used as the shortened forms of the source and the source mask of 0.0.0.0 0.0.0.0.
source-mask	Stands for the source address of the network mask. The keyword any is used as the shortened forms of the source and the source mask of 0.0.0.0 0.0.0.0.
destination	Stands for the destination network or host number. There are two methods to designate this parameter: A decimal number separated by four points and a 32-bit binary number. The keyword any is used as the shortened forms of the destination and the destination mask of 0.0.0.0 0.0.0.0.
destination-mask	Stands for the destination address of the network mask. The keyword any is used as the shortened forms of the destination address and the destination mask of 0.0.0.0 0.0.0.0.
precedence *precedence*	Filters the packets based on the precedence. The precedence of the packet can be designated by an integer from 0 to 7. This parameter is optional.
tos *tos*	An optional parameter, meaning that the packets can be filtered at the service layer. It is designated by any number between 0 and 15. Its value ranges between 0 and -15.
icmp-type	It is an optional parameter which means that the ICMP packets can be filtered by the ICMP message type. The type is presented by a number between 0 and 255.

igmp-type	It is an optional parameter which means that the ICMP packets can be filtered by the ICMP type or packet name. The type is presented by a number between 0 and 15.
operator	((Optional) Compares the source or destination ports.) The operations include lt, gt, eq and neq. If the operator symbol is behind source and source-mask, it must match up the source port. If the operator symbol is behind destination and destination-mask, it must match up the destination port.
Port	(Optional) Stands for a decimal number or name of the TCP/UDP port. The port number is a value between 0 and 65535. The name of the TCP port is listed in the Usage Explanation part. When the TCP is filtered, only the name of the TCP port can be used. The names of the UDP ports are also listed in the Usage Explanation part. When the TCP is filtered, only the name of the TCP port can be used. When the UDP is filtered, only the name of the UDP port can be used.
established	An optional parameter for the TCP protocol, representing an established connection. If the TCP data reports that the ACK or RST is configured, the match-up appears. For the unmatched case, the TCP packet is initialized to establish a connection.
log	An optional parameter, meaning the logs can be recorded
location	Insert the rule to designated num

Command Mode

IP ACL configuration commands

Usage Guidelines

The virtual terminal path access can be controlled and the content of the routing update can be limited through the transmission of the ACL control packet on the interface. After the matchup occurs, the expanded access control list will not be checked again. The IP segment, not the initial segment, is received by any extended IP access control list. The extended IP access control list is used to control the virtual terminal's acess path or limit the content of the routing update, however, it need not to match up with the source TCP port, the type of the service value or the priority of the packets.

Note:

After an access control list is originally established,(ny added content is)put at the end of the list.

The following are the names of the TCP port. For reference of these protocols, see RFC of these protocols. You can search the corresponding port number of these protocols by entering a question mark behind the relative command.

Bgp、ftp、ftp-data、login、pop2、pop3、smtp、telnet、www

The following are the names of the UDP port. For reference of these protocols, see RFC of these protocols. You can search the corresponding port number of these protocols by entering a question mark behind the relative command.

Domain, snmp,syslog, tftp

Example

The following example shows how to forbid network segment 192.168.5.0.

ip access-list standard filter

deny 192.168.5.0 255.255.255.0

Note:
The IPaccess control listdenyends with a connotative deny regulation.

Related Command

ip access-group
ip access-list
permit
show ip access-list

3.2.2 ip access-group

Syntax

To control and access an interface, run ip access-group. To delete the designated access group, run no ip access-group {access-list-name}{in | out}.
ip access-group {*access-list-name*}{**in** | **out**}
no ip access-group {*access-list-name*}{**in** | **out**}

Parameters

Parameters	Description
access-list-name	Stands for the name of an access control list. This is a character string with up to 20 characters.
In	Uses the access control list on the incoming interface.
out	Uses the access control list on the outgoing interface.

Command Mode

Interface configuration mode

Usage Guidelines

The access control list can be used on the incoming or outgoing interface. After a packet is received, the source address of the packet will be checked according to the standard egress interface access control list. For the expanded access control list, the switch also checks the destination address. If the access control list permits the destination address, the system will continue handling the packet. However, if the access control list forbids the destination address, the system will drop the packet and then returns an ICMP unreachable packet.
For the standard access list of the out interfaces, after a packet is received or routed to the control interface, the software checks the source address of the packet according to the access list. For the

expanded access control list, the switch will also check the access control list at the receiver terminal. If the access list permits the address, the software will send the packet. If the access list does not permit the address, the software drops the packet and returns an ICMP unreachable message.
If the designated access control list does not exist, all packets are allowed to pass through.

Example

The following example shows how to apply the filter list on the exgress port of Ethernet interface vlan1.

interface vlan 1

ip access-group filter out

Related Command

ip access-list
show ip access-list

3.2.3 ip access-list

Syntax

After this command is run, the system enters the IP ACL configuration mode. In this mode, you can add and delete the access regulations. You can run exit to return the configuration mode.
You can run no ip access-list to delete the IP access control list.
ip access-list {**standard** | **extended**} *name*
no ip access-list {**standard** | **extended**} *name*

Parameters

Parameters	Description
standard	Designates a standard access control list.
extended	Designates an extended access control list.
name	Stands for the name of an access control list. It is a character string with up to 20 characters.

Default Value

No IP access control list is defined by default.

Command Mode

Global configuration mode

Usage Guidelines

This command is used to enter the IP ACL configuration mode and then you can use the deny command and the permit command to configure the access regulation.

Example

The following example shows how to configure a standard IP access control list.

ip access-list standard filter

deny 192.168.1.0 255.255.255.0

permit any

Related Command

deny
ip access-group
permit
show ip access-list

3.2.4 permit

Syntax

To configure the permit reglation in IP ACL configuration mode, run permit. To cancel the permit reglation, run no permit.
permit source [*source-mask*] **[log] [location]**
no permit source [*source-mask*] **[log]**
permit protocol source *source-mask* **destination** *destination-mask* [[**precedence** precedence] [**tos** tos] [**log] [offset-zero] [totallen] [time-range] [location] [ttl] [donotfragment-set] [donotfragment-notset] [is-fragment] [not-fragment] [offset-not-zero] [log**]]
no permit protocol source *source-mask* **destination** *destination-mask* [[**precedence** precedence] [**tos** tos] [**log] [offset-zero] [totallen] [time-range] [location] [ttl] [donotfragment-set] [donotfragment-notset] [is-fragment] [not-fragment] [offset-not-zero] [log**]]
For the Internet Control Message Protocol (ICMP), use the following command syntax.
permit icmp source *source-mask* **destination** *destination-mask* [*icmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log**]
For the Internet Group Management Protocol (IGMP), run the following command syntax.
permit igmp source *source-mask* **destination** *destination-mask* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**log**]
For the Transmission Control Protocol (TCP), use the following command syntax.
permit tcp source *source-mask* [**operator** *port*] **destination** *destination-mask* [**operator** *port*] [**established**] [**precedence** *precedence*] [**tos** tos] [log]
For the User Datagram Protocol (UDP), use the following command syntax.

permit udp source *source-mask* [**operator port** [*port*]] **destination** *destination-mask* [**operator** *port]* [**precedence** *precedence*] [**tos** *tos*] [**log**]

Parameters

Parameters	Description
protocol	Stands for the protocol name or IP protocol number. It can be icmp, igmp, igrp, ip, ospf, tcp or udp, or it can be an integer from 0 to 255 which stands for the IP protocol. To match up any Internet protocol, including ICMP, TCP and UDP, you can use the ip keyword. Some protocols allow further limitations as described below.
source	Stands for a source network or host number. There are two methods to designate the source: 32-bit binary number or a decimal number separated by four points. The keyword any is used as the shortened forms of the source and the source mask of 0.0.0.0 0.0.0.0.
source-mask	Stands for the source address of the network mask. The keyword any is used as the shortened forms of the source and the source mask of 0.0.0.0 0.0.0.0.
destination	Stands for the destination network or host number. There are two methods to designate this parameter: A decimal number separated by four points and a 32-bit binary number. The keyword any is used as the shortened forms of the destination and the destination mask of 0.0.0.0 0.0.0.0.
destination-mask	Stands for the destination address of the network mask. The keyword any is used as the shortened forms of the destination address and the destination mask of 0.0.0.0 0.0.0.0.
precedence *precedence*	Filters the packets based on the precedence. The precedence of the packet can be designated by an integer from 0 to 7. This parameter is optional.
tos *tos*	An optional parameter, meaning that the packets can be filtered at the service layer. It is designated by any number between 0 and 15. Its value ranges between 0 and -15.
icmp-type	It is an optional parameter which means that the ICMP packets can be filtered by the ICMP message type. The type is presented by a number between 0 and 255.
igmp-type	It is an optional parameter which means that the ICMP packets can be filtered by the ICMP type or packet name. The type is presented by a number between 0 and 15.
operator	((Optional) Compares the source or destination ports.) The operations include lt, gt, eq and neq. If the operator symbol is behind source and source-mask, it must match up the source port. If the operator symbol is behind destination and destination-mask, it must match up the destination port.
Port	(Optional) Stands for a decimal number or name of the TCP/UDP port. The port number is a value between 0 and 65535. The name of the TCP port is listed in the Usage Explanation part. When the TCP is filtered, only the name of the TCP port can be used. The names of the UDP ports are also listed in the Usage Explanation part. When the TCP is filtered, only the name of the TCP port can be used. When the UDP is filtered, only the name of the UDP port can be used.
established	An optional parameter for the TCP protocol, representing an established connection. If the TCP data reports that the ACK or RST is configured, the match-up appears. For the unmatched case, the TCP packet is initialized to establish a connection.
log	An optional parameter, meaning the logs can be recorded

Command Mode

IP ACL configuration commands

Usage Guidelines

The virtual terminal path access can be controlled and the content of the routing update can be limited through the transmission of the ACL control packet on the interface. After the matchup occurs, the expanded access control list will not be checked again.
The IP segment, not the initial segment, is received by any extended IP access control list. The extended IP access control list is used to control the virtual terminal's acess path or limit the content of the routing update, however, it need not to match up with the source TCP port, the type of the service value or the priority of the packets.
Note:
After an access control list is originally established,(ny added content is)put at the end of the list.
The following are the names of the TCP port. For reference of these protocols, see RFC of these protocols. You can search the corresponding port number of these protocols by entering a question mark behind the relative command.
Bgp、ftp、ftp-data、login、pop2、pop3、smtp、telnet、www
The following are the names of the UDP port. For reference of these protocols, see RFC of these protocols. You can search the corresponding port number of these protocols by entering a question mark behind the relative command.
Domain, snmp, syslog, tftp

Example

The following example shows how to allow network segment 192.168.5.0.

ip access-list standard filter

permit 192.168.5.0 255.255.255.0

Note:
The IP access control list deny ends with a connotative deny regulation.

Related Command

deny
ip access-group
ip access-list
show ip access-list

3.2.5 show ip access-list

Syntax

To display the content of the current IP access control list, run the following command.

show ip access-list [*access-list-name*]

Parameters

Parameters	Description
access-list-name	Stands for the name of an access control list. It is a character string with up to 20 characters.

Default Value

This command is used to display all standard and extended IP access control lists.

Command Mode

EXEC

Usage Guidelines

The command helps you to designate a specific access control list.

Example

The following information is displayed when the show ip access-list command is run in case an IP access control list is designated.

Switch# show ip access-list

ip access-list standard aaa

permit 192.2.2.1

permit 192.3.3.0 255.255.255.0

ip access-list extended bbb

permit tcp any any eq www

permit ip any any

The following information is displayed when the show ip access-lists bbb command is run in case that an access control list is designated.

ip access-list extended bbb

permit tcp any any eq www

permit ip any any

3.3 IP ACL based on physical port

The commands for configuring the IP Access Control List (ACL) are:

- deny
- ip access-group

- ip access-list
- permit
- show ip access-list

3.3.1 deny

Syntax

To configure the deny reglations in IP ACL configuration mode, run deny source [source-mask] or deny protocol source source-mask destination destination-mask [tos tos]. To remove a deny regulation from an IP ACL, run no deny source [source-mask] or no deny protocol source source-mask destination destination-mask [tos tos].

deny source [*source-mask*] **[log] [location]**

no deny source [*source-mask*] [**log**]

deny protocol source source-mask destination destination-mask [[**precedence** precedence] [**tos** tos] [**log] [offset-zero] [totallen] [time-range] [location] [ttl] [donotfragment-set] [donotfragment-notset] [is-fragment] [not-fragment] [offset-not-zero] [log**]]

no deny protocol source source-mask destination destination-mask [[**precedence** precedence] [**tos** tos] [**log] [offset-zero] [totallen] [time-range] [location] [ttl] [donotfragment-set] [donotfragment-notset] [is-fragment] [not-fragment] [offset-not-zero] [log**]]

For the Internet Control Message Protocol (ICMP), use the following command syntax.

deny icmp source source-mask destination destination-mask [icmp-type] [**tos** tos]

For the Internet Group Management Protocol (IGMP), run the following command syntax.

deny igmp source source-mask destination destination-mask [igmp-type] [**tos** tos]

For the Transmission Control Protocol (TCP), use the following command syntax.

deny tcp source source-mask [operator port] destination destination-mask [operator port] [**tos** tos]

For the User Datagram Protocol (UDP), use the following command syntax.

deny udp source source-mask [operator port] destination destination-mask [operator port] [**tos** tos]

Parameters

Parameters	Description
protocol	Stands for the protocol name or IP protocol number. It can be icmp, igmp, igrp, ip, ospf, tcp or udp, or it can be an integer from 0 to 255 which stands for the IP protocol. To match up any Internet protocol, including ICMP, TCP and UDP, you can use the ip keyword. Some protocols allow further limitations as described below.
source	Stands for a source network or host number. There are two methods to designate the source: 32-bit binary number or a decimal number separated by four points. The keyword any is used as the shortened forms of the source and the source mask of 0.0.0.0 0.0.0.0.
source-mask	Stands for the source address of the network mask. The keyword any is used as the shortened forms of the source and the source mask of 0.0.0.0 0.0.0.0.

destination	Stands for the destination network or host number. There are two methods to designate this parameter: A decimal number separated by four points and a 32-bit binary number. The keyword any is used as the shortened forms of the destination and the destination mask of 0.0.0.0 0.0.0.0.
destination-mask	Stands for the destination address of the network mask. The keyword any is used as the shortened forms of the destination address and the destination mask of 0.0.0.0 0.0.0.0.
tos *tos*	An optional parameter, meaning that the packets can be filtered at the service layer. It is designated by any number between 0 and 15. Its value ranges between 0 and -15.
icmp-type	It is an optional parameter which means that the ICMP packets can be filtered by the ICMP message type. The type is presented by a number between 0 and 255.
igmp-type	It is an optional parameter which means that the ICMP packets can be filtered by the ICMP type or packet name. The type is presented by a number between 0 and 15.
operator	((Optional) Compares the source or destination ports.) The operations include eq, gt, lt and portrange. If the operator symbol is behind source and source-mask, it must match up the source port. If the operator symbol is behind destination and destination-mask, it must match up the destination port.
Port	(Optional) Stands for a decimal number or name of the TCP/UDP port. The port number is a value between 0 and 65535.

Command Mode

IP ACL configuration commands

Usage Guidelines

The virtual terminal path access can be controlled and the content of the routing update can be limited through the transmission of the ACL control packet on the interface. After the matchup occurs, the expanded access control list will not be checked again. The IP segment, not the initial segment, is received by any extended IP access control list. The extended IP access control list is used to control the virtual terminal's acess path or limit the content of the routing update, however, it need not to match up with the source TCP port, the type of the service value or the priority of the packets.

Note:

After an access control list is originally established,(ny added content is)put at the end of the list.

Example

The following example shows how to forbid network segment 192.168.5.0.

ip access-list standard filter

deny 192.168.5.0 255.255.255.0

Note:

The IPaccess control listdenyends with a connotative deny regulation.

Related Command

ip access-group
ip access-list
permit
show ip access-list

3.3.2 ip access-group

Syntax

To control and access an interface, run ip access-group {access-list-name}{in | out}. To delete the designated access group, run no ip access-group {access-list-name}{in | out}.
[no] ip access-group [*access-list-name*]

Parameters

Parameters	Description
access-list-name	Stands for the name of an access control list. This is a character string with up to 20 characters.

Command Mode

Interface configuration mode

Usage Guidelines

The access control list is used on the incoming interface. After a packet is received, the source address of the packet will be checked according to the standard egress interface access control list. For the expanded access control list, the switch also checks the destination address. If the access control list permits the destination address, the system will continue handling the packet. However, if the access control list forbids the destination address, the system will drop the packet and then returns an ICMP unreachable packet.
If the designated access control list does not exist, all packets are allowed to pass through.

Example

The following example shows how to apply the filter list on the ingress port of Ethernet interface g0/10:

```
interface g0/10
ip access-group filter
```

Related Command

ip access-list
show ip access-list

3.3.3 ip access-list

Syntax

After this command is run, the system enters the IP ACL configuration mode. In this mode, you can add and delete the access regulations. You can run exit to return the configuration mode.
You can run no ip access-list to delete the IP access control list.
ip access-list {**standard** | **extended**} *name*
no ip access-list {**standard** | **extended**} *name*

Parameters

Parameters	Description
standard	Designates a standard access control list.
extended	Designates an extended access control list.
name	Stands for the name of an access control list. It is a character string with up to 20 characters.

Default Value

No IP access control list is defined by default.

Command Mode

Global configuration mode

Usage Guidelines

This command is used to enter the IP ACL configuration mode and then you can use the deny command and the permit command to configure the access regulation.

Example

The following example shows how to configure a standard IP access control list.

ip access-list standard filter

deny 192.168.1.0 255.255.255.0

permit any

Related Command

deny
ip access-group
permit
show ip access-list

3.3.4 permit

Syntax

To configure the permit regulations in IP ACL configuration mode, run permit. To cancel the permit regulations, run no permit.
permit source [*source-mask*] **[log] [location]**
no permit source [*source-mask*] **[log]**
permit protocol source *source-mask* **destination** *destination-mask* [[**precedence** precedence] [**tos** tos] [**log] [offset-zero] [totallen] [time-range] [location] [ttl] [donotfragment-set] [donotfragment-notset] [is-fragment] [not-fragment] [offset-not-zero] [log**]]
no permit protocol source *source-mask* **destination** *destination-mask* [[**precedence** precedence] [**tos** tos] [**log] [offset-zero] [totallen] [time-range] [location] [ttl] [donotfragment-set] [donotfragment-notset] [is-fragment] [not-fragment] [offset-not-zero] [log**]]
For the Internet Control Message Protocol (ICMP), use the following command syntax.
permit icmp source *source-mask* **destination** *destination-mask* [*icmp-type*] [**tos** *tos*]
For the Internet Group Management Protocol (IGMP), run the following command syntax.
permit igmp source *source-mask* **destination** *destination-mask* [*igmp-type*] [**tos** *tos*]
For the Transmission Control Protocol (TCP), use the following command syntax.
permit tcp source *source-mask* [**operator** *port*] **destination** *destination-mask* [**operator** *port*] [**tos** tos]
For the User Datagram Protocol (UDP), use the following command syntax.
permit udp source *source-mask* [**operator port** [*port*]] **destination** *destination-mask* [**tos** *tos*]

Parameters

Parameters	Description
protocol	Stands for the protocol name or IP protocol number. It can be icmp, igmp, igrp, ip, ospf, tcp or udp, or it can be an integer from 0 to 255 which stands for the IP protocol. To match up any Internet protocol, including ICMP, TCP and UDP, you can use the ip keyword. Some protocols allow further limitations as described below.
source	Stands for a source network or host number. There are two methods to designate the source: 32-bit binary number or a decimal number separated by four points. The keyword any is used as the shortened forms of the source and the source mask of 0.0.0.0 0.0.0.0.
source-mask	Stands for the source address of the network mask. The keyword any is used as the shortened forms of the source and the source mask of 0.0.0.0 0.0.0.0.

destination	Stands for the destination network or host number. There are two methods to designate this parameter: A decimal number separated by four points and a 32-bit binary number. The keyword any is used as the shortened forms of the destination and the destination mask of 0.0.0.0 0.0.0.0.
destination-mask	Stands for the destination address of the network mask. The keyword any is used as the shortened forms of the destination address and the destination mask of 0.0.0.0 0.0.0.0.
tos *tos*	An optional parameter, meaning that the packets can be filtered at the service layer. It is designated by any number between 0 and 15. Its value ranges between 0 and -15.
icmp-type	It is an optional parameter which means that the ICMP packets can be filtered by the ICMP message type. The type is presented by a number between 0 and 255.
igmp-type	It is an optional parameter which means that the ICMP packets can be filtered by the ICMP type or packet name. The type is presented by a number between 0 and 15.
operator	((Optional) Compares the source or destination ports.) The operations include eq, gt, lt and portrange. If the operator symbol is behind source and source-mask, it must match up the source port. If the operator symbol is behind destination and destination-mask, it must match up the destination port.
Port	(Optional) Stands for a decimal number or name of the TCP/UDP port. The port number is a value between 0 and 65535.

Command Mode

IP ACL configuration commands

Usage Guidelines

The virtual terminal path access can be controlled and the content of the routing update can be limited through the transmission of the ACL control packet on the interface. After the matchup occurs, the expanded access control list will not be checked again.

The IP segment, not the initial segment, is received by any extended IP access control list. The extended IP access control list is used to control the virtual terminal's acess path or limit the content of the routing update, however, it need not to match up with the source TCP port, the type of the service value or the priority of the packets.

Note:

After an access control list is originally established,(ny added content is)put at the end of the list.

Example

The following example shows how to allow network segment 192.168.5.0.

ip access-list standard filter

permit 192.168.5.0 255.255.255.0

Note:

The IP access control list deny ends with a connotative deny regulation.

Related Command

deny
ip access-group
ip access-list
show ip access-list

3.3.5 show ip access-list

Syntax

To display the content of the current IP access control list, run the following command.
show ip access-lists [*access-list-name* **[config-list | merge-list | both-list]**]

Parameters

Parameters	Description
access-list-name	Stands for the name of an access control list. It is a character string with up to 20 characters.
config-list	Displays the original config list.
merge-list	Displays the merge list.
both-list	Displays the config list and the merge list.

Default Value

This command is used to display all standard and extended IP access control lists.

Command Mode

EXEC

Usage Guidelines

The command helps you to designate a specific access control list.

Example

The following information is displayed when the show ip access-list command is run in case an IP access control list is designated.

Switch# show ip access-list

ip access-list standard aaa

permit 192.2.2.1

permit 192.3.3.0 255.255.255.0

ip access-list extended bbb

permit tcp any any eq 25

permit ip any any

The following information is displayed when the show ip access-lists bbb command is run in case that an access control list is designated.

ip access-list extended bbb

permit tcp any any eq 25

permit ip any any

https://www.fs.com

The information in this document is subject to change without notice. FS has made all efforts to ensure the accuracy of the information, but all information in this document does not constitute any kind of warranty.

Copyright © 2009-2022 FS.COM All Rights Reserved.