Network Protocol Configuration Commands

Table of Contents

Chapter 1 **IP Addressing Configuration Commands**

1.1 IP Addressing Configuration Commands

IP addressing configuration commands include:

- arp
- arp scan
- arp timeout
- clear arp-cache
- ip address
- ip directed-broadcast
- ip forward-protocol udp
- ip helper-address
- ip host
- ip proxy-arp
- ip unnumbered
- keepalive
- show arp
- show hosts
- show ip interface

1.1.1 arp

To configure the static ARP which will permanently be stored in the ARP cache, run **arp [vrf *vrf-name*] *ip-address hardware-address* [alias]**. To delete the configured static ARP, run **no arp [vrf *vrf-name*] *ip-address***.

arp [**vrf** *vrf-name*] *ip-address hardware-address* [**alias**]

no arp [**vrf** *vrf-name*] *ip-address*

Parameter

Parameter	Description

Vrf-name	VRF name (for the VRF version)
ip-address	IP address of the local link interface
hardware-address	Physical address of the local link interface
alias	(optional) the router will answer the ARP request from the IP address.

Default

No permanent static ARP mapping exists in the ARP cache.

Command Mode

Global configuration mode

Instruction

A common host can support the dynamic ARP resolution; hence, you need not specially configure the static ARP mapping for the host. The **vrf** subcommand is used to specify which VRF the ARP item belongs to.

Example

The following command 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

Related Command

clear arp-cache

1.1.2 arp timeout

To configure the timeout value of the dynamic ARP item in the ARP cache, run **arp timeout seconds**. To resume the default value of the ARP item, run **no arp timeout** or **default arp timeout**.

arp timeout seconds

no arp timeout

default arp timeout

Parameter

Parameter	Description

seconds	Timeout value of the dynamic ARP item in the ARP cache. 0 means that the ARP cache obtained through dynamic resolution on the port will not be released at the timeout time

Default

14400seconds (4 hours)

Command Mode

Interface configuration mode

Instruction

If the timeout value of the dynamic ARP item is configured on the non-arp interface, the configuration is invalid. You can run show interface to display the timeout time of the ARP items on the port. See the following information :

ARP type: ARPA, ARP timeout 04:00:00

Example

The following example shows that the timeout time of the dynamic ARP mapping on interface Ethernet 1/0 is set to 900 seconds, which enables the ARP cache to be refreshed rapidly.

```
!
interface ethernet 1/0
arp timeout 900
!
```

Related Command

show interface

1.1.3 clear arp-cache

To delete all dynamic ARP cache, run the following command:

clear arp-cache

Parameter

The command has no parameters or keywords.

Command Mode

EXEC

Example

The following command is used to delete all dynamic ARP cache.

clear arp-cache

Related Command

arp

1.1.4 ip address

To configure the IP address of the interface and the network mask simultaneously, run **ip address**. Currently, the IP addresses can not be clearly classified into A type, B type and C type. However, the multicast address and the broadcast address can not be used(The host part is 1.). Except the Ethernet, multiple interfaces of other types of network can work on the same network segment. The network segment configured by the Ethernet interface cannot be same to that configured by other types of interfaces, unnumbered interfaces excluded. One main address and multiple accessory addresses can be configured on an interface. The accessory address can be configured only after the main address is configured, while the main address can be deleted only after all accessory addresses are deleted. If the upper-layer application does not specify the source address of the system-generated IP packet, the router will adopt the IP address (configured on the transmitter interface and is in the same network segment as the gateway); if the IP address cannot be determined, the main address of the transmitter interface will be adopted. If the IP address of an interface is not configured and the interface is not an unnumbered interface, the IP packets will not be handled on the interface.

To delete an IP address or stop the IP packets from being handled on an interface, run **no ip address**.

ip address *ip-address mask* [**secondary**]

no ip address *ip-address* **mask**

no ip address

Parameter

Parameter	Description
ip-address	IP address
mask	Mask of the IP network
secondary	(optional) specifies an accessory IP address. If the IP address is not specified, it must be a main IP address.

Default

No IP addresses is configured on the interface.

Command Mode

Interface configuration mode

Instruction

If you configure the accessory IP address on a physical network segment through the router, you must configure the accessory IP address of the same logical network segment for other systems on the same physical network segment; otherwise, the routing loop will be easily generated.

When the OSPF protocol is used, make sure that the accessory address and the main address of an interface must be in the same OSPF area.

Example

The following example shows that the main address on interface Ethernet1/0 is set to 202.0.0.1, network mask is set to 255.255.255.0 and two accessory IP addresses are set to 203.0.0.1 and 204.0.0.1 respectively.

```
interface ethernet1/0
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
```

1.1.5 ip directed-broadcast

To forward the directed IP broadcast and transmit the packets in the physical broadcast form, run **IP directed-broadcast [access-list-namer]**.

ip directed-broadcast [*access-list-namer*]

no ip directed-broadcast

Parameter

Parameter	Description
access-list-name	Name of the access list, which is an optional parameterIf the access list is defined, only broadcast packets permitted by the access list can be forwarded.

Default

The directed IP broadcast will not be forwarded by default.

Command Mode

Interface configuration mode

Example

The following example shows how to configure the directed IP broadcast forwarding on interface Ethernet1/0.

```
!
interface ethernet 1/0
ip directed-broadcast
!
```

1.1.6 ip forward-protocol udp

To specify which UDP packets to be forwarded after IP helper-address is configured on the interface, run **ip forward-protocol udp [*port*]**.

ip forward-protocol udp [*port*]

no ip forward-protocol udp [*port*]

default ip forward-protocol udp

Parameter

Parameter	Description
ISDN(BRI)	(optional) destination port which the to-be-forwarded UDP packets is transmitted to

Default

The NETBIOS Name Service packet is forwarded.

Command Mode

Global configuration mode

Instruction

The NETBIOS Name Service packet is forwarded by default; to stop forwarding the NETBIOS Name Service packet, run either of the following two commands:

no ip forward-protocol udp netbios-ns

no ip forward-protocol udp 137

To stop forwarding all UDP packets, run the following command:

no ip forward-protocol udp

Example

Router_config#ip forward-protocol udp 137

Related Command

ip helper-address

1.1.7 ip helper-address

To forward the directed IP packets to the designated IP helper address (unicast address or broadcast address), run **ip helper-address**. You can configure multiple helper addresses on each interface.**ip helper-address** *address*

no ip helper-address [*address*]

Parameter

Parameter	Description
address	IP helper address

Default

The IP helper address is not configured.

Command Mode

Interface configuration mode

Instruction

The command is invalid on the X.25 interface, because the router cannot identify physical broadcasts.

Example

The following example shows how to set the IP helper address on interface ethernet1/0 to 1.0.0.1.

!

interface ethernet 1/0

ip helper-address 1.0.0.1

!

Related Command

ip forward-protocol udp

1.1.8 ip host

To define a static host name-to-address mapping in the host cache, use the **ip host** command in global configuration mode. To remove the host name-to-address mapping, use the no form of this command.

ip host *name address*

no ip host *name*

parameter parameter	description
name	Host name
Address	IP address

Default

No mapping is configured.

Command Mode

Global configuration

Example

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

ip host dns-server 202.96.1.3

1.1.9 ip proxy-arp

To enable the agent ARP on the interface, run **ip proxy-arp**. To disable the agent ARP on the interface, run **no ip proxy-arp**.

ip proxy-arp

no ip proxy-arp

Parameter

The command has no parameters or keywords.

Default

The agent ARP is conducted.

Command Mode

Interface configuration mode

Instruction

When the router receives the ARP request, if the router has the route to the requested IP address and the routing interface is different from the request-received interface, the router will send the ARP response out through its own MAC address; after then, the actual data packet will be forwarded after it is received. In this way, a host can communicate with the remote host even if the host does not completely learn the network topology or the correct router is not set for the host. The host is in the same physical subnet as a remote host is.

If a host requires the router to provide the service, the host and the router must be in the same IP network, or at least the router takes that the IP address of the host and the router are in the same IP subnet, that is, they use different masks. The router, otherwise, cannot provide the service.

Example

The following example shows how to enable the ARP agent on interface ethernet1/0.

```
!
interface ethernet 1/0
ip proxy-arp
!
```

1.1.10 ip unnumbered

To set an interface to an unnumbered interface to enable the IP process function without configuring the IP address, run **ip unnumbered *type number***. To stop the IP process on the interface, run **no ip unnumbered**.

ip unnumbered *type number*

no ip unnumbered

Parameter

Parameter	Description
type number	Type and number of an interface whose IP address is configured The interface cannot be the unnumbered interface which has adopted the IP address of other interfaces.

Default

The function is disabled.

Command Mode

Interface configuration mode

Instruction

You need not configure the unique IP address for the point-to-point link interface. You can run the command to directly handle the IP and specify the valid IP address of other interfaces as the source address of the packets transmitted from the interface. The IP address is thus saved. The point-to-point interface can be called as the unnumbered interface. IP packets generated on the unnumbered interface, such as route-refresh packets, will use the valid IP addresses configured on the command-designated interface. The address must be used to determine which routing processes are sending the refresh packets on the interface. However, it has the following limitations:

(1) The command can set serial interfaces/channel interfaces that are encapsulated by HDLC, PPP, LAPB and SLIP to unnumbered interfaces. However, the command cannot be used on the X.25 interface and the SMDS interface.

(2) You cannot check whether the interface works normally through the ping command. However, you can use SNMP to check the state of the interface remotely.

The command realizes its function based on the regulation in RFC 1195 that the valid IP address cannot be configured on the interface.

Pay attention to the serial links (between different networks) that adopt the IP address of other interfaces; any routing protocol running on the serial link cannot broadcast any information about each subnet.

Example

The following example shows how to set interface serial0/0 to an unnumbered interface and adopt the valid IP address, 1.0.0.1, which configured on interface ethernet0/1, as the source address of the packet transmitted from the interface.

```
!
interface ethernet 0/1
ip address 1.0.0.1 255.255.255.0
!
interface serial 0/0
ip unnumbered ethernet 1/0
!
```

1.1.11 keepalive

To test the reachablity of the host and the connectivity of the network, run the following command:

keepalive [**group** *group-id*] [**source** *source-address*] [**interval** interval-time] [**number** *number*] **destination** *destination-address*

Parameter

Parameter	Description
group *group-id*	Multiple **keepalive** commands can be configured and can be identified by the group ID. The default value of the group ID is 0.
source *source-address*	Specifies the source IP address adopted by the packet. Default: the main IP address of the transmitted interface
interval *interval-time*	Interval for transmitting the packet, whose unit is second Default value: 1 second
number *number*	Number of the transmitted packets Its default value is 5.
destination *destination-address*	Destination host

Command Mode

EXEC or global configuration mode

Instruction

The **keepalive** command supports the broadcast address and the multicast address. If the address is the limited broadcast address (255.255.255.255) or the multicast address, the ICMP response packet will be transmitted on all interfaces supporting broadcasts and multicasts.

The command need not wait for the ICMP response packet, which only transmits the designated number of ICMP packets to the destination address regularly.

Example

The following shows that two **keepalive** commands are configured.

You can make a configuration that 10 ICMP request packets are transmitted from source address 192.168.20.230 to destination address 192.168.20.1 every 10 seconds. The packet-transmitting port is determined through destination address 192.168.20.1 and the routing protocol.

keepalive group 1 destination 192.168.20.1 source 192.168.20.230 interval 10 number 10

You can make a configuration that five ICMP request packets are transmitted from source address 172.16.20.232 to destination address 172.16.20.5 every second. The

packet-transmitting port is determined through destination address 172.16.20.2 and the routing protocol.

keepalive group 2 destination 172.16.20.2 source 172.16.20.232

1.1.12 ip route-cache-timeout

The command is to configure route cache timeout value (aging time).

(no)ip route-cache-timeout *timeout-value*

Parameter

Parameter	Parameter Description
timeout-value	Route cache timeout value. Unit: 5 seconds, default: 1 (timeout-value is 5 seconds)

Command Mode

Global configuration

Instruction

The command is to set route timeout value. The longer the route timeout value, the shorter the same data flow (source address and destination address are the same.). When the data flow is small (less than 10000) and stable, prolong the route timeout value appropriately can improve the route forwarding rate. However, when the data flow is big (over 10000) and unstable, prolong the timeout value may reduce the route forwarding rate. It is recommended to adopt the default value (it is, the user spares the trouble to set the route timeout value). For 1705 broadband routers of our company, it is recommended to set the route timeout value to 16 (80 seconds) in two-way mode.

Example

The following command is to set the route cache timeout value to 10 seconds.

router#config
router_config#
router_config#ip route-cache-timeout 2

The following command is to delete the configuration of the route cache timeout value as 10 seconds:

router#config
router_config#
router_config#no ip route-cache-timeout 2

Then the route cache timeout value resumes to the default value 1.

1.1.13 show arp

To display all ARP items, including the ARP mapping of the IP address for the interface, static ARP mapping and dynamic ARP mapping, run the following command:

show arp [**vrf** *vrf-name*]

Parameter

None

Command Mode

EXEC

Instruction

The displayed information shows in the following table:

Parameter	Description
Protocol	Protocol type, such as the IP protocol
Address	Address type, such as the IP address
Age	Lifetime, that is, the duration of ARP item from its generation (unit: minute) The fact that the router uses the ARP item does not affect the value.
Hardware Address	Physical address corresponding to the network address, which is null for the unresolved item
Type	Type of packet encapsulation used by the interface, including ARPA and SNAP
Interface	Interface relative with the network address

Example

The following command is used to display the ARP cache.

```
router#show arp
Protocol    IP Address        Age(min)   Hardware Address     Type   Interface
IP          192.168.20.77       11     00:30:80:d5:37:e0    ARPA   Ethernet1/0
IP          192.168.20.33        0         Incomplete
IP          192.168.20.22        -     08:00:3e:33:33:8a    ARPA   Ethernet1/0
IP          192.168.20.124       0     00:a0:24:9e:53:36    ARPA   Ethernet1/0
IP          192.168.0.22         -     08:00:3e:33:33:8b    ARPA   Ethernet1/1
```

1.1.14 show hosts

To display all items in the hostname-address cache, run the following command:

show hosts

Parameter

The command has no parameters or keywords.

Command Mode

EXEC

Example

The following example shows how to display all hostname-address mappings:

show ip hosts

Related Command

clear host

1.1.15 arp learn-strict

Run **arp learn strict** to set “arp learn strict”. Run **no arp learn-strict** To disable the function.

arp learn-strict

no arp learn-strict

Parameter

None

Default

Disable arp learn-strict

Mode

Interface configuration

Instruction

Enable arp learn-strict and prevent ARP attack: the host will update the route ARP item continuously.

Example

The following example shows how to enable ARP learn-strict:

Router_config_g0/0#arp learn-strict

1.1.16 arp source-filter

Run **arp source-filter** to set ARP source address filtration. Run **no arp source-filter** to resume to the default mode.

arp source-filter

no arp source-filter

Parameter

None

Default

Disable ARP source address filtration.

Command Mode

Port configuration

Instruction

Enable ARP source address filtration to check route according to the ARP source address. If the destination port is not the port, ARP packet will be dropped.

Example

The following example shows how to enable ARP source address filtration.

Router_config_g0/0#arp source-filter

1.1.17 arp timeout

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

Parameter

<10-4294967>

Default

180seconds

Command Mode

Interface configuration

Instruction

Modify the aging time (timeout) of ARP

Example

The following example shows how to enable arp timeout as 10s.

```
Router_config_g0/0#arp timeout 10
```

1.1.18 arp dynamic

To set arp learning dynamic, run **arp dynamic**. To disable the function, run **no arp dynamic**.

arp dynamic

no arp dynamic

Parameter

None

Default

Enable ARP dynamic learning

Command Mode

Port configuration

Instruction

Enable ARP dynamic learning, receive ARP packet and update ARP table according to the source address IP & MAC.

Example

The following example shows how to disable ARP dynamic learning:

Router_config_g0/0#no arp dynamic

1.1.19 arp proxy

To set route ARP, run **arp proxy <all | range>**. To disable the function, run **no arp proxy <all | range>** to disable the function.

arp proxy <all | range>

no arp proxy <all | range>

Parameter

All: proxy all IP addresses

Range: designated IP address range of ip & mask.

Default

Disable ARP

Command Mode

Port configuration

Instruction

Enable ARP and the route will response ARP request of Proxy IP.

Example

The following example shows how to set ARP proxy.

Router_config_g0/0#arp proxy all

1.1.20 arp scan

To set route ARP scan, run **arp scan <all | range>**. To disable the function.run **no arp scan <all | range>**.

arp scan <all | range>

no arp scan <all | range>

Parameter

All:scan all IP addresses

Range: designated IP address range of ip & mask.

Default

Disable ARP scan

Command Mode

Port configuration

Instruction

Enable ARP scan. The route will actively request for the IP address within the scan range and formulate static ARP item.

Example

The following example shows how to set ARP scan:

```
Router_config_g0/0#arp scan all
```

1.1.21 arp guard

To set route ARP anti-attack, run **arp guard**. To disable the function, run **no arp guard**.

arp guard

no arp guard

Parameter

None

Default

Disable ARP guard

Command Mode

Interface configuration

Instruction

Enable ARP guard, check its validity and drop the illegal packet.

Example

The following example shows how to set ARP guard:

```
Router_config_g0/0#arp guard
```

1.1.22 arp guard rate-limit

To set route ARP packet rate limit, run **arp guard rate-limit <num>**. To disable the function, run **no arp guard rate-limit**.

arp guard rate-limit <num>

no arp guard rate-limit

Parameter

Number of ARP received every second

Default

1000

Command Mode

Interface configuration

Instruction

Enable ARP rate limit, calculate number of ARP and drop ARP packet exceeding the threshold.

Example

The following example shows how to set ARP attack prevention.

```
Router_config_g0/0#arp guard rate-limit 500
```

1.1.23 arp free-arp

To set route forward free ARP regularly, run **arp free-arp <time>**. To disable the function, run **no arp free-arp**.

arp free-arp <time>

no arp free-arp

Parameter

0~600 (0.1s)

Default

Forward free ARP irregularly.

Command Mode

Port configuration

Instruction

Enable forward free ARP regularly.

Example

The following example shows how to set forward ARP regularly:

```
Router_config_g0/0#arp free-arp 100
```

1.1.24 arp <ip><mac>

To set route static ARP, run **arp <ip> <mac>**. To disable the function, run **no arp <ip> <mac>**.

arp <ip> <mac>

no arp <ip> <mac>

Parameter

The format of Ip: a.b.c.d

The format of Mac: hh:hh:hh:hh:hh:hh

Default

None

Command Mode

Global configuration

Instruction

Enable static ARP: the route will not request for ARP of IP and the state will not be modified.

Example

The following example shows how to set static ARP:

```
Router_config#arp 1.1.1.1 00:a0:0c:13:64:7d
```

1.1.25 show arp

Show ARP item.

Show arp

Parameter

None

Default

None

Command Mode

Global configuration

Instruction

Show the current ARP item.

Example

The following example shows how to show ARP item:

```
Router_config#show arp

##'M': manual 'B':bind 'S':static 'D':dynamic##
There are 1 ARP Entries Totally
Proto Address          Age(s) Hardware Address     Type    Interface
IP    1.1.1.160        -      00:a0:0c:13:64:7d    --D     GigaEthernet0/1
```

1.1.26 clear arp

Clear ARP item.

Show arp

Parameter

None

Default

None

Command Mode

Global configuration

Instruction

Clear current ARP item.

Example

The following example shows how to clear ARP item:

Router_config#clear arp

1.1.27 show ip interface

To display the IP configuration of the interface, run the following command:

show ip interface [*type number*]

Parameter

Parameter	Description
type	Type of the interface, which is optional
number	Number of the interface, which is optional

Command Mode

EXEC

Instruction

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 router 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 that the IP configuration of interface e0/1 is displayed.

Router#show ip interface e0/1
Ethernet1/0 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

The following table gives a detailed description to some parameters in the previous example.

Domain	Description
Ethernet1/0 is up	If the hardware of the interface is available, the interface will be identified as **up**. If the interface is available, its hardware and line protocols must be in the **up** state.
line protocol is up	If the interface can provide bidirectional communication, the line protocol will be identified as **up**. If the interface is available, its hardware and line protocols of the interface must be in the **up** state.
IP address	IP address of an interface and network mask
Broadcast address	Displays the broadcast address.
MTU	Displays the IP MTU configured on the interface.
Helper address	Displays the IP 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 router.
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 **NAT Configuration Commands**

2.1 NAT Configuration Commands

NAT configuration commands include:

- ip nat
- ip nat local-service
- ip nat enable-peek
- ip nat inside destination
- ip nat inside source
- ip nat outside source
- ip nat pool
- ip nat translation
- clear ip nat statistics
- clear ip nat translation
- show ip nat statistics
- show ip nat translations
- debug ip nat

2.1.1 ip nat

ip nat {**inside | outside | mss inside | outside | mss** }

no ip nat {**inside | outside | mss *MSS-value***}

Parameter

Parameter	Description
inside	Shows that the interface connects the internal network (NAT is applied on the network).
outside	Shows that the interface connects the exterior network (NAT is applied on the network).
mss *MSS-value*	Sets MSS to **MSS-value** after **ip nat outside** must be configured.

Default

The communication volume transmitted or received by the interface does not obey the NAT regulation.

Command Mode

Interface configuration mode

Instruction

Only the packets forwarded between interior interfaces and exterior interfaces can be translated. Each boundary router where the NAT function is applied must be specified at least one interior interface and one exterior interface.

You can run IP NAT to specify that the communication volume coming from the interface or transmitted to the interface obeys NAT; to forbid the NAT function on the interface, run **no IP nat**.

Note:

The **ip nat mss** command can be configured only on the interface of **IP NAT outside**. Its function is to modify the maximum segment size (MSS) in the synchronous TCP packets that are transmitted from the interior network. To forbid the interface to modify MSS, run **no ip nat mss**.

Example

The following example shows that the IP address of packets from host 192.168.1.0 or host 192.168.2.0 is translated to the unique IP address of network 171.69.233.208/28 and MSS is modified to 1432.

```
!
ip nat pool net-208 171.69.233.208 171.69.233.223 255.255.255.240
ip nat inside source list a1 pool net-208
!
interface ethernet 0
ip address 171.69.232.182 255.255.255.240
ip nat outside
 ip nat mss 1432
!
interface ethernet 1
ip address 192.168.1.94 255.255.255.0
ip nat inside
!
ip access-list standard a1
permit 192.168.1.0 255.255.255.0
permit 192.168.2.0 255.255.255.0
!
```

2.1.2 ip nat local-service

ip nat local-service {**icmp** | **udp** | **tcp** } **disable**

no ip nat local-service {**icmp** | **udp** | **tcp** } **disable**

Parameter

Parameter	Description
icmp	Icmp packet
udp	Udp packet
tcp	Tcp packet

Default

None

Command Mode

Interface configuration mode

Instruction

The command is used to the NAT regulations. By default, all ICMP/UDP/TCP packets to access the local router are permitted on the router's interface which is identified as the NAT exterior port. The command can limitedly prevent exterior network users from viciously attack the router; however, the packets which normally access the router will be dropped.

To forbid the local ICMP/UDP/TCP packets to access the local router through the router's interface which is identified as the NAT exterior port, you need configure the **ip nat local-service** {**icmp** | **udp** | **tcp** } **disable** command. You can use the “no” form of the command to resume the default state.

Note:

The command can be configured only on the router’s interface where the NAT-identified exterior port lies and can be used to disable only the interface to receive the ICMP/UDP/TCP packets.

2.1.3 ip fastaccess

ip fastaccess deny {**tcp** | **udp** | **icmp**} {***port*** *number*}

no ip fastnat deny {**tcp** | **udp** | **icmp**} {***port*** *number*}

Parameter

Parameter	Description
deny	Defines the regulations of the **deny** packets.
tcp	Defines the regulations of the **tcp** packets.
udp	Defines the regulations of the **udp** packets.
icmp	Defines the regulations of the **icmp** packets.
Port number	Number of the TCP/UDP port, ranging between 1 and 10000

Default

None

Command Mode

Interface configuration mode

Instruction

Because the **ip fastaccess** command is used to limit packet forwarding on the basis of the transmission layer, the general access list will be used if packet forwarding is limited based on the IP address.

Note:

If you want to constrain interior users through general access lists in the premises of using dynamic NAT regulations, you are strongly recommended to use the NAT-adopted access list. This method can greatly improve the performance especially for the access lists which require to define many regulations.

2.1.4 ip fastnat 1to1

ip fastnat 1to1 outside {***interface****-type number*} [**backup-outside** {***interface-****type number*}] **inside** {***interface-****type number*} [**privateservices**] [**extend**]

no ip fastnat

Parameter

Parameter	Description
outside ***interface-****type number*	Designated network interface which is identified as NAT OUTSIDE, which is the exit of the main line
backup-outside ***interface-****type number*	Designated network interface which is identified as NAT INSIDE, which is the exit of the backup line
inside interface type number	Designated network interface which is identified as NAT INSIDE, which is the entrance of the backup

	line
privateservices	(optional) Enables the private service.
extend	(optional) Enables the expanded access list.

Default

None

Command Mode

Global configuration mode

Instruction

The command has requirements for network environment. For details, see the configuration manual.

If the private service or expanded access control list is not used, do not use the **privateservices** option or the **extend** option.

2.1.5 ip nat inside destination

To enable the NAT of the interior destination address, run **ip nat inside destination**. To delete the dynamic connection with the address pool, run **no ip nat inside destination**.

ip nat inside destination list *access-list-name* **pool** *name*

no ip nat inside destination list *access-list-name*

Parameter

Parameter	Description
list name	Name of the standard IP access control list, which is used to translate the packets with the destination address through the global address in the designated address pool
pool name	Name of the address pool During the dynamic translation, the address pool will distribute interior local IP addresses.

Default

The interior destination address is not translated.

Command Mode

Global configuration mode

Instruction

The command is used to create the dynamic address translation in the access control list form. For the packets from the address matched with the standard access control list, the global address allocated by the designated address pool will be used to translate. The address pool is specified by the **ip nat pool** command.

Example

The following example shows that the packets from network 171.69.233.208 are translated to the address of the interior host whose destination address lies at network segment 192.168.2.208.

```
!
ip nat pool net-208 192.168.2.208 192.168.2.223 255.255.255.240
ip nat inside destination list a1 pool net-208
!
interface ethernet 0
ip address 171.69.232.182 255.255.255.240
ip nat outside
!
interface ethernet 1
ip address 192.168.1.94 255.255.255.0
ip nat inside
!
ip access-list standar a1
permit 171.69.233.208 255.255.255.240
!
```

2.1.6 ip nat inside source

To enable the NAT of the interior source address, run ip nat inside source**. To delete the static translation or the dynamic connection with the address pool, run** no ip nat inside source**.**

Note： Dynamic NAT regulations and static network-segment NAT regulations cannot be deleted if they are being used.

Dynamic NAT:

ip nat inside source {**list** *access-list-name*} {**interface** *type number* | **pool** *pool-name*} [**overload**]

no ip nat inside source {**list** *access-list-name*} {**interface** *type number* | **pool** *pool-name*} [**overload**]

Static NAT for a single address:

ip nat inside source {**static** {*local-ip global-ip*}

no ip nat inside source {**static** {*local-ip global-ip*}

Static port NAT:

ip nat inside source {**static** {**tcp** | **udp** *local-ip local-port* {*global-ip* | **interface** *type number*} *global-port*}

no ip nat inside source {**static** {**tcp** | **udp** *local-ip local-port* {*global-ip* | **interface** *type number*} *global-port*}

Static NAT of the network segment:

ip nat inside source {**static** {**network local-network global-network** *mask*}

no ip nat inside source {**static** {**network local-network global-network** *mask*}

Parameter

Parameter	Description
List access-list-name	Name of the IP access control list The packets whose source addresses matches the access control list will be translated by the global address of the address pool.
pool name	Name of the address pool where the global IP addresses are dynamically distributed
interface type number	Specifies the network interface.
overload	(optional) enables the router to use one global address for multiple local addresses. After the overload parameter is set, multiple sessions of similar hosts or different hosts will be differentiated by TCP numbers or UDP numbers.
static local-ip	Creates an independent static address translation. It is a local IP address which is distributed to the interior hosts. The local IP address can be selected freely or distributed from RFC 1918.
local-port	Sets the local TCP/UDP number, ranging between 1 and 65535.
static global-ip	Creates independent static address translation. That is, it is used to create an IP address through which an exterior network can access uniquely.
global-port	Sets the global TCP/UDP number, ranging between 1 and 65535.
tcp	Sets TCP port translation.
udp	Sets UDP port translation.

network local-network	Sets the translation for the local network segment.
global-network	Sets the translation for the global network segment.
mask	Sets the network mask for the network segment translation.

Default

The NAT of any interior source address does not exist.

Command Mode

Global configuration mode

Instruction

The command has two modes: dynamic address translation and static address translation. The dynamic translation is created for the access control list form. For the packets from the address matched with the standard access control list, the global address allocated by the designated address pool will be used to translate. The address pool is specified by the **ip nat pool** command.

As a secondary method, the syntax format with keyword STATIC need an independent static address translation to be created.

To enable the static NAT to support the PASV mode of FTP, those commands to match the overload type are required. When a static FTP mapping of NAT is set, the overload type transfer is needed and one of the addresses of the exterior-network interface following the PAT regulations must be the same as the exterior-network address of the static FTP.

Example

The following example shows that the IP address of packets from host 192.168.1.0 or host 192.168.2.0 is translated to the unique IP address of network 171.69.233.208/28.

```
!
ip nat pool net-208 171.69.233.208 171.69.233.223 255.255.255.240
ip nat inside source list a1 pool net-208
!
interface ethernet 0
ip address 171.69.232.182 255.255.255.240
ip nat outside
!
interface ethernet 1
ip address 192.168.1.94 255.255.255.0
ip nat inside
!
ip access-list standard a1
permit 192.168.1.0 255.255.255.0
```

permit 192.168.2.0 255.255.255.0
!

The following is an example of using the PASV mode of the static FTP.

ip nat inside source static tcp 10.1.1.1 21 204.112.1.2 8021
ip nat inside source static tcp 10.1.1.1 20 204.112.1.2 8020
ip nat inside source list test1 interface f0/0

2.1.7 ip nat outside source

To enable the NAT of the exterior source address, run **ip nat outside source**. To delete the static items or dynamic connection, run **no ip nat outside source**.

Note： Dynamic NAT regulations and static network-segment NAT regulations cannot be deleted if they are being used.

Dynamic NAT:

ip nat outside source {**list** *access-list-name*} **pool** *pool-name*

no ip nat outside source {**list** *access-list-name*} **pool** *pool-name*

Static NAT for a single address:

ip nat outside source static {*global-ip local-ip*}

no ip nat outside source static {*global-ip local-ip*}

Static port NAT:

ip nat outside source {**static** {**tcp** | **udp** *global-ip global-port local-ip local-port*}

no ip nat outside source {**static** {**tcp** | **udp** *global-ip global-port local-ip local-port*}

Static NAT of the network segment:

ip nat outside source {**static network** *global-network local-network mask*}

no ip nat outside source {**static network** *global-network local-network mask*}

Parameter

Parameter	Description
List access-list-name	Name of the standard IP access control list The packets whose source addresses matches the access control list will be translated by the global address of the address pool.。
pool name	Name of the address pool where the global IP addresses are dynamically distributed
Static global-ip	Creates an independent static address translation. It is a global IP address which is distributed by the hosts creating the exterior network. The address can be distributed in the globally-routing

	network address space.
global-port	Sets the global TCP/UDP number, ranging between 1 and 65535.
Static local-ip	Creates independent static address translation. That is, it is used to create an local IP address of the exterior host through which an interior network can access uniquely. The address can be distributed in the address space which can be routed by the interior network.
local-port	Sets the local TCP/UDP number, ranging between 1 and 65535.
tcp	Sets TCP port translation.
udp	Sets UDP port translation.
network global-network	Sets the translation for the global network segment.
local-network	Sets the translation for the local network segment.
mask	Sets the network mask for the network segment translation.

Default

The translation between the source addresses of the exterior network and the interior network address does not exist.

Command Mode

Global configuration mode

Instruction

You probably use the illegal and abnormally-distributed IP address. You also probably use the IP address which is normally distributed to other networks. The fact that the IP address is legally used by the exterior network and also illegally used by the interior network is defined as address overlapping. The NAT can be used to translate the interior addresses which are overlapped with the exterior addresses. If the IP address of your single-connection network is same to the legal IP address of another network and you need communicate with these hosts or routers, you can use the function.

The command has two modes: dynamic address translation and static address translation. The dynamic translation is created for the access control list form. For the packets from the address matched with the standard access control list, the local address allocated by the designated address pool will be used to translate. The address pool is specified by the **ip nat pool** command.

As a secondary method, the syntax format with keyword STATIC need an independent static address translation to be created.

Example

The following example shows that the IP address of packets among hosts in network 9.114.11.0 is translated to the unique global IP address of network 171.69.233.208/28.

Further more, the IP address of packets among hosts in network 9.114.11.0 (an authentic 9.114.11.0 network) is translated to the network 10.0.1.0/24.

```
!
ip nat pool net-208 171.69.233.208 171.69.233.223 255.255.255.240
ip nat pool net-10 10.0.1.0 10.0.1.255 255.255.255.0
ip nat inside source list a1 pool net-208
ip nat outside source list a1 pool net-10
!
interface ethernet 0
ip address 171.69.232.182 255.255.255.240
ip nat outside
!
interface ethernet 1
ip address 9.114.11.39 255.255.255.0
ip nat inside
!
ip access-list standard a1
permit 9.114.11.0 255.255.255.0
 !
```

2.1.8 ip nat pool

To define an IP address pool for NAT, run **ip nat pool**. To delete the IP address pool with a designated name, run **no ip nat pool**.

ip nat pool name *start-ip end-ip netmask* [**rotary**]

no ip nat pool *name*

Parameter

Parameter	Description
name	Name of the IP address pool
start-ip	Start IP address for defining the range of the IP address pool
end-ip	End IP address for defining the range of the IP address pool
netmask	Subnet mask showing which bytes belong to the network and subnet and which bytes belong to the host parts; it can be used to specify the subnet mask of the network to which the addresses of the IP address pool belongs.
rotary	Rotary address pool

Default

The IP address pool is not defined.

Command Mode

Global configuration mode

Instruction

The command is used to define an IP address pool with the start IP address, end IP address and subnet mask.

Note: The rotary regulations of the IP address pool in the PAT regulations are shown in the following: only when all connections of an address are aging, the next address is required. That is, there is only one interior global address at the same time.

Example

The following example shows that the IP address of packets from host 192.168.1.0 or host 192.168.2.0 is translated to the unique IP address of network 171.69.233.208/28.

```
!
ip nat pool net-208 171.69.233.208 171.69.233.223 255.255.255.240
ip nat inside source list a1 pool net-208
!
interface ethernet 0
ip address 171.69.232.182 255.255.255.240
ip nat outside
!
interface ethernet 1
ip address 192.168.1.94 255.255.255.0
ip nat inside
!
ip access-list standard a1
permit 192.168.1.0 255.255.255.0
permit 192.168.2.0 255.255.255.0
!
```

2.1.9 ip nat service

The command is an entrance function provided for all services that NAT supports. Currently, only three kinds of services are provided. All services are disabled by default.

ip nat service { **h323** | **privateservice** | **peek** }

no ip nat service { **h323** | **privateservice** | **peek** }

Parameter

None

Default

Shut down

Command Mode

Global configuration mode

Instruction

The command is used to control the NAT support of h323.

Private service is a kind of support that the NAT does to the internal game server of the cyber bar, such as the legend. It can control the NAT support of the private service.

The **peek** parameter realizes the NAT support to the game monitor server in the cyber bar. Through the client soft of , you can monitor internal users' surfing.

The “no” form of the command is used to disable corresponding functions.

Example

ip nat service privateservice
ip nat service peek
ip nat service h323
no ip nat service peek

2.1.10 ip nat translation

You can run **ip nat translation** to do the following:

Modifying the timeout value of the NAT translation. You can run **no ip nat translation** to close the timeout.

ip nat translation {**timeout** | **udp-timeout** | **dns-timeout** | **tcp-timeout** | **finrst-timeout** | **icmp-timeout** | **syn-timeout** } *seconds*

no ip nat translation {**timeout** | **udp-timeout** | **dns-timeout** | **tcp-timeout** | **finrst-timeout** | **icmp-timeout** | **syn-timeout** }

Modifying the values of some parameters for NAT translation items. You can use the “no” form of the command to delete the previous configuration or resume the default values.

ip nat translation max-entries { **host** [*A.B.C.D* | **any]** } *numbers*

no ip nat translation max-entries { **host** [*A.B.C.D* | **any**] }

Parameter

Parameter	Description

Timeout	Specifies the timeout value of the dynamic translations except the overload translation. The default value is 3600 seconds.
udp-timeout	Specifies the timeout value for the UDP port. The default value is 300 seconds.
dns-timeout	Specifies the timeout value to connect the DNS. The default value is 60 seconds.
tcp-timeout	Specifies the timeout value for the TCP port. The default value is 3600 seconds.
finrst-timeout	Specifies the timeout value of the **finish and reset TCP** message, which is used to terminate a translation item. The default value is 60 seconds.
icmp-timeout	Sets the timeout time of the NAT of ICMP; the default value is 60 seconds.
max-entries	Sets the maximum number of the NAT translation items; the default value is 3000.
syn-timeout	Sets the NAT timeout time of the TCP SYN state; the default value is 60 seconds.
seconds	Specifies the timeout value of the port translation. The default value is the value listed out at the default part.
max-entries host *A.B.C.D*	For the specified internal IP address, you can control the maximum number of the NAT translation items. There is no default value. You can use the “no” form of the command not to control the maximum number of the NAT translation items.
max-entries host any	For all internal IP addresses, the maximum number of the NAT translation items can be controlled by limiting the single IP address. The default value is same to max-entries.

Default

timeout is 3600 seconds (1 hours)

udp-timeout is 300 seconds (5 minutes)

dns-timeout is 60 seconds (1 minute)

tcp-timeout is 3600 seconds (1 hours)

finrst-timeout is 60 seconds (1 minute)

Command Mode

Global configuration mode

Instruction

After the port translation is configured, you can further control the translation items for each translation item contains more information about the communication volume. The

UDP translation of the DNS times out five minutes later, while that of the domain system times out one minute later. If there is no RST or FIN in the data flow, TCP translation times out one hour later; if there is RST or FIN, it will time out one minute later.

Example

Example 1:

The following example shows that the UDP port translation times out 10 minutes later.

ip nat translation udp-timeout 600

Example 2:

The following example shows that the maximum number of the NAT translation items created by IP 192.168.20.1 is set to 100.

ip nat translation max-entries host 192.168.20.1 100

2.1.11 clear ip nat statistics

To delete the NAT statistics information, run **clear ip nat statistics**.

clear ip nat statistics

Parameter

None

Command Mode

EXEC

Instruction

You can use the command to resume all NAT statistics information to the original state.

Note:

Only the statistics parameter behind the **packets dropped** option can be deleted.

Example

Router#show ip nat statistics

Total active translations: 2 (1 static, 0 dynamic, 1 PAT)
Outside interfaces:

FastEthernet0/1

Inside interfaces:

FastEthernet0/0

Dynamic mappings:
--Inside Source
access-list nat
pool natp: netmask 255.255.255.0
start 172.16.20.125 end 172.16.20.127
total addresses 3, misses 0
--Inside Destination
--Outside Source
Link items:

PAT(ICMP=5 UDP=39 TCP=224 / TOTAL=268), Dynamic=6

Packets dropped:
--Protocol:
Out: tcp 123, udp 39, icmp 10, others 6
In: tcp 46, udp 109, icmp 0, others 10
--Configuration:
max entries 0, max entries for host 178
Router#clear ip nat statistics
Router#show ip nat statistic
Total active translations: 2 (1 static, 0 dynamic, 1 PAT)
Outside interfaces:

FastEthernet0/1

Inside interfaces:

FastEthernet0/0

Dynamic mappings:
--Inside Source
access-list nat
pool natp: netmask 255.255.255.0
start 172.16.20.125 end 172.16.20.127
total addresses 3, misses 0
--Inside Destination
--Outside Source
Link items:

PAT(ICMP=5 UDP=39 TCP=224 / TOTAL=268), Dynamic=6

Packets dropped:
--Protocol:
Out: tcp 0, udp 0, icmp 0, others 0
In: tcp 0, udp 0, icmp 0, fragments 0
--Configuration:
max entries 0, max links for host 0

2.1.12 clear ip nat translation

To delete dynamic NAT from the translation item, run the following commands:

clear ip nat translation {***** | [**inside** local-ip global-ip] [**outside** local-ip global-ip]}

clear ip nat translation {**tcp|udp**} **inside** *local-ip local-port global-ip global-port* [**outside** *local-ip global-ip*]

Parameter

Parameter	Description
*	Deletes all dynamic translation items.
Inside	Deletes the internal translation consisting of the global IP address and the local IP address.
global-ip	Specifies the global IP address.
local-ip	Specifies the local IP address.
outside	Deletes the external translation consisting of the designated global IP address and the local IP address.
tcp|udp	Protocol
global-port	Specifies the global port for the corresponding protocol.
local-port	Specifies the local port for the corresponding protocol.

Command Mode

EXEC

Instruction

You can run the command to delete the dynamic translation items before they time out.

Example

The following example shows that the NAT translation items are displayed first and then the UDP translation items are deleted.

```
Router# show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
udp 171.69.233.209:1220 192.168.1.95:1220 171.69.2.132:53    171.69.2.132:53
tcp 171.69.233.209:11012 192.168.1.89:11012 171.69.1.220:23  171.69.1.220:23
tcp 171.69.233.209:1067 192.168.1.95:1067 171.69.1.161:23    171.69.1.161:23
Router# clear ip nat translation udp inside 171.69.233.209 1220 192.168.1.95 1220
171.69.2.132 53 171.69.2.132 53
Router# show ip nat translation
```

Pro Inside global Inside local Outside local Outside global
tcp 171.69.233.209:11012 192.168.1.89:11012 171.69.1.220:23 171.69.1.220:23
tcp 171.69.233.209:1067 192.168.1.95:1067 171.69.1.161:23 171.69.1.161:23

2.1.13 show ip nat statistics

To display the NAT statistics table, run **show ip nat statistics**.

show ip nat statistics

Parameter

The command has no parameters or keywords.

Command Mode

EXEC

Example

The following information is displayed after you run **show ip nat statistics**.

Router# show ip nat statistics
Total active translations: 2 (1 static, 0 dynamic, 1 PAT)
Outside interfaces:
FastEthernet0/1
Inside interfaces:
FastEthernet0/0
Dynamic mappings:
--Inside Source
access-list nat
pool natp: netmask 255.255.255.0
start 172.16.20.125 end 172.16.20.127
total addresses 3, misses 0
--Inside Destination
--Outside Source
Link items:
PAT(ICMP=0 UDP=5 TCP=24 / TOTAL=29), Dynamic=0
Packets dropped:
--Protocol:
Out: tcp 0, udp 0, icmp 0, others 0
In: tcp 46, udp 100, icmp 0, others 0
--Configuration:
max entries 0, max links for host 0

The important fields in the output results are listed in table 2-1.

Table 2- 1 Field description of show ip nat statistics

Field	Description
Total active translations:	Number of designated translations activated in the system When an address translation regulation is created, the value increases by 1; when an address translation regulation is deleted or times out, the value decreases by 1.
Outside interfaces:	List of outside interfaces which are identified by the **ip nat outside** command.
Inside interfaces:	List of inside interfaces which are identified by the **ip nat inside** command.
Dynamic mappings:	Information about dynamic mapping
Inside Source:	Information about the inside source address translation
Access-list	Number of access lists for address translation
Pool	Name of the address pool
Netmask	IP network mask used by the address pool
Start	Start IP address of the address range
End	End IP address of the address range
Total addresses	Number of addresses in the pool, which can be used for address translation
Misses	Number of addresses which cannot be distributed from the address pool
Inside Destination:	Information about the inside destination address translation
Outside Source:	Information about the outside source address translation
Link items:	Number and type of translation items
PAT	Number of translation items under dynamic port translation regulations, among which **madia** stands for the RTP/RTCP session.
Dynamic	Number of translation items under dynamic address translation regulations including FTP-created translation items translated from static addresses
Packets dropped:	Type, number and reason of the dropped packets
Protocol	Number, protocol type and NAT direction of the dropped packets
Configuration	Number of packets which are dropped for an incorrect reason: **max entries** means that the maximum number of translation items is exceeded; **max links for host** means that the number of translation items permitted by each address or a specific address is exceeded.

2.1.14 show ip nat translations

To display the activated NAT address translation, run **show ip nat translations**.

show ip nat translations [**host *A.B.C.D* | tcp** | **udp** | **icmp** | **verbose**]

Parameter

Parameter	Description
host *A.B.C.D*	(optional) Displays translation items A, B, C and D which have the inside local address.
tcp	(optional) Displays translation items which bear the TCP session.
udp	(optional) Displays translation items which bear the TCP session.
icmp	(optional) Displays translation items which bear the ICMP session.
Verbose	(optional) Displays extra information about each translation item, including how long it has been created and how long it times out.

Command Mode

EXEC

Instruction

Example

The following information is displayed after you run **show ip nat translations**.

Two inside hosts and some outside hosts are switching packets without overload.

```
Router# show ip nat translations
Pro Inside local      Inside global     Outside local     Outside global
--- 192.168.1.95      171.69.233.209    ---               ---
--- 192.168.1.89      171.69.233.210    ---               --
```

(3) The following example shows that, at the overload condition, three address translation items are activated, among which one is for DNS and the other two are for the TELNET session. **Note**: two different inside hosts can appear with the same outside address.

```
Router# show ip nat translations
Pro Inside local      Inside global        Outside local      Outside global
udp 192.168.1.95:1220 171.69.233.209:1220  171.69.2.132:53    171.69.2.132:53
tcp 192.168.1.89:11012 171.69.233.209:11012 171.69.1.220:23   171.69.1.220:23
tcp 192.168.1.95:1067 171.69.233.209:1067  171.69.1.161:23    171.69.1.161:23
```

The following example shows the information with the **verbose** keyword.

```
Router# show ip nat translations verbose
Pro Inside local      Inside global     Outside local      Outside global
```

udp 192.168.1.95:1220 171.69.233.209:1220 171.69.2.132:53 171.69.2.132:53
create time 00:00:02 , left time 00:01:10 ,
tcp 192.168.1.89:11012 171.69.233.209:11012 171.69.1.220:23 171.69.1.220:23
create time 00:01:13 , left time 00:00:50 ,
tcp 192.168.1.95:1067 171.69.233.209:1067 171.69.1.161:23 171.69.1.161:23
create time 00:00:02 , left time 00:53:19 ,

Table 2- 2 Fields of output results for the **show IP NAT Translations** command

Field	Description
Pro	Defines the port protocol of the address.
Inside global	Legal IP address, standing for one or multiple inside local IP addresses connecting the exterior network
Inside local	IP address which is allocated to the inside host It may not a legal address provided by NIC or SP.
Outside local	IP address of an outside host when it looks like an inside network, which may not be a legal address provided by NIC or SP
Outside global	IP address of the outside host which is distributed by the owner
Create time	Creation time of the translation item (its unit is hour: minute: second)
Left time	Timeout time of the address translation

2.1.15 debug ip nat

To debug NAT, run **debug ip nat**.

debug ip nat {**detail** | **h323**}

no debug ip nat {**detail** | **h323**}

Parameter

None

Command Mode

EXEC

Instruction

You can **run debug ip nat detail** to export the details about the translation procedure, including the source/destination IP address, port number and the reason of the failed translation.

You also can run **debug ip nat h323** to export the details about the NAT translation of the H323 packets, including the H323 information identified by NAT, the IP address of the message or the translated address for the inside address.

Example

Example 1:

Router# debug ip nat detail

Ethernet1/1 recv ICMP Src 194.4.4.89 Dst 10.10.10.102 no link found

Ethernet1/0 send TCP Src 194.4.4.102:2000 Dst 192.2.2.1:21 no matched rule

Table 2- 3 Fields in the previous example

Field	Description
Ethernet1/0	Type and number of the interface
send/recv	Send/receive
ICMP/TCP/UDP	ICMP/TCP/UDP protocol
Src 194.4.4.102:2000	Source IP address and port number
Dst 192.2.2.1:21	Destination IP address and port number
no link found	Means that the NAT translation item is not matched.
no matched rule	Means that the NAT regulations are not matched.

The first command line shows that the ICMP packets (the source address is 194.4.4.89, the destination address is 10.10.10.102; ICMP) are received by interface Ethernet1/1 and the corresponding NAT translation items are not found.

The second command line shows that the TCP packets (the source address is 194.4.4.102, the destination address is 192.2.2.1; the source port is 2000, the destination port is 21) are transmitted from interface Ethernet1/0 and the matched NAT regulations are not found.

Example 2:

Router# debug ip nat h323

NAT:H225:[I] processing a Setup message

NAT:H225:[I] found Setup sourceCallSignalling

NAT:H225:[I] fix TransportAddress addr-192.168.122.50:11140

NAT:H225:[I] found Setup fastStart

NAT:H225:[I] Setup fastStart PDU length:18

NAT:H245:[I] processing OpenLogicalChannel message, forward channel 1

NAT:H245:[I] found OLC forward mediaControlChannel

NAT:H245:[I] fix TransportAddress addr-192.168.122.50:16517

NAT:H225:[I] Setup fastStart PDU length:29

NAT:H245:[I] processing OpenLogicalChannel message, forward channel 1

NAT:H245:[I] found OLC reverse mediaChannel

NAT:H245:[I] fix TransportAddress addr-192.168.122.50:16516

NAT:H245:[I] found OLC reverse mediaControlChannel

NAT:H245:[O] fix TransportAddress addr-192.168.122.50:16517

NAT:H225:[O] processing an Alerting message
NAT:H225:[O] found Alerting fastStart
NAT:H225:[O] Alerting fastStart PDU length:25
NAT:H245:[O] processing OpenLogicalChannel message, forward channel 1

The important fields are described in the following table.

Field	Description
NAT	Means the packet has been translated by NAT.
RAS/H255/H245	Protocol type of the packet
O	Transmission direction of the packet: inside to outside
I	Transmission direction of the packet: outside to inside

Chapter 3 **DHCP Client Configuration Commands**

3.1 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

3.1.1 ip address dhcp

To obtain an IP address for the Ethernet interface through DHCP, run **ip address dhcp**. To delete the obtained IP address, run **no ip address dhcp**.

ip address dhcp

no ip address dhcp

Parameter

None

Default

None

Command Mode

Interface configuration mode

Instruction

The **ip address dhcp** command allows the interface to obtain the IP address through the DHCP protocol, which is useful for dynamically connecting the Internet service provider (ISP) through the Ethernet interface. Once the dynamic IP address is obtained, the Ethernet interface can adopt the PAT technology to realize the network address translation (NAT).

If the **ip address dhcp** command is configured on the router, the router will transmit the DHCPDISCOVER message to the DHCP server.

If the **no ip address dhcp** command is configured on the router, the router will transmit the DHCP RELEASE message.

Example

The following example shows that interface Ethernet1/1 obtains its IP address through the DHCP protocol.

```
!
interface Ethernet1/1
ip address dhcp
!
```

Related Command

ip dhcp client

ip dhcp-server

show dhcp lease

show dhcp server

3.1.2 ip dhcp client

To configure the parameter about the DHCP client of the local router, run **ip dhcp client**.

ip dhcp client { **minlease seconds | retransmit count | select seconds** }

no ip dhcp client { **minlease | retransmit | select** }

Parameter

Parameter	Description
minlease seconds	(optional) the minimum lease time, ranging from 60 to 86400 seconds
retransmit *count*	(optional) retransmit times of the protocol packets, ranging between 1 and 10
retry_interval	(optional) Interval for retriggering the DHCP request, ranging between 1 and 1440 minutes
select *seconds*	(optional) interval for the **select** operation, ranging between 0 and 30

Default

The default value of the **minlease** parameter is 60 seconds.

The default value of the **retransmit** parameter is four times.

The default value of the **retry-interval** parameter is five seconds.

The default value of the **select** parameter is 0 seconds.

Command Mode

Global configuration mode

Instruction

You can adjust these parameters according to the network structure and the DHCP server's requirements.

If the "no" forms of these commands are configured, the parameters are reset to the default values defined by the system.

Example

The following example shows that the receivable minimum lease time of the DHCP client on the router is set 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 to three times.

```
ip dhcp client retransmit 3
```

The following example shows how to set the interval of retriggering the DHCP request on the DHCP client to 10 minutes.

```
ip dhcp client retry_interval 10
```

The following example shows how to set the interval of selecting on the DHCP client to 10 seconds.

```
ip dhcp client select 10
```

Related Command

ip address dhcp

ip dhcp-server

show dhcp lease

show dhcp server

3.1.3 ip dhcp-server

To specify the IP address of the DHCP server, run **ip dhcp-server**.

ip dhcp-server *ip-address*

no ip dhcp-server *ip-address*

Parameter

Parameter	Description
ip-address	IP address of the DHCP server

Default

The default IP address of the DHCP server does not exist.

Command Mode

Global configuration mode

Instruction

The command can be used to specify the IP address of the DHCP server, while the previously-designated IP address of the DHCP server will not be replaced.

You can use the “no” form of the command to delete the previously-configured IP address of the DHCP server.

Example

The following example shows how to set the server with IP 192.168.20.1 to the DHCP server.

ip dhcp-server 192.168.20.1

Related Command

ip address dhcp

ip dhcp client

show dhcp lease

show dhcp server

3.1.4 show dhcp lease

To check the DHCP server distribution information used by the current router, run **show dhcp lease**.

Show dhcp lease

Parameter

None

Default

None

Command Mode

EXEC

Instruction

The command can be used to check the DHCP server distribution information used by the current router.

Example

The following example shows the DHCP server distribution information used by the router.

```
router#show dhcp lease
Temp IP addr: 192.168.20.3    for peer on Interface: Ethernet1/1
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-Et1/1
```

Related Command

ip address dhcp

ip dhcp client

ip dhcp-server

show dhcp server

debug dhcp

3.1.5 show dhcp server

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

show dhcp server

Parameter

None

Default

None

Command Mode

EXEC

Instruction

The command is used to display the information about the known DHCP server.

Example

The following example shows the information about the known DHCP server.

```
router#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

3.1.6 debug dhcp

To check the treatment condition of the DHCP protocol, run **debug dhcp**.

debug dhcp <detail>

no debug dhcp <detail>

Parameter

Parameter	Description
detail	Displays the content of the DHCP packet.

Default

Relative information will not be displayed by default.

Command Mode

EXEC

Instruction

The following example shows some important information about DHCP treatment:

router#debug dhcp
router#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 Ethernet1/1 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 DHCP: B'cast on Ethernet1/1 interface from 0.0.0.0
2000-4-22 10:50:54 DHCP: SDISCOVER attempt # 3, sending 277 byte DHCPpacket

Related Command

show dhcp lease

Chapter 4 **DHCP Server Configuration Commands**

4.1 DHCP Server Configuration Commands

DHCP server configuration commands include:

- ip dhcpd ping packet
- ip dhcpd ping timeout
- ip dhcpd write-time
- ip dhcpd database-agent
- ip dhcpd pool
- ip dhcpd enable
- ip dhcpd disable

4.1.1 ip dhcpd ping packet

ip dhcpd ping packet *pkgs*

Parameter

Parameter	Description
pkgs	A parameter used by the DHCP server to check whether the address has distributed the number of the transmitted ICMP packets.

Default

2

Command Mode

Global configuration mode

Instruction

You can run the following command to configure whether the DHCP server has transmitted **n** ICMP packets when it check whether the address is distributed.

ip dhcpd ping packets *n*

Example

You can run the following command to configure whether the DHCP server has transmitted **n** ICMP packets when it check whether the address is distributed.

ip dhcpd ping packets 1

4.1.2 ip dhcpd ping timeout

Parameter

Parameter	Description
timeout	Timeout time for waiting the ICMP echo message when the DHCP server is used to check whether the address is distributed (unit: 100 ms)

Default

5

Command Mode

Global configuration

Instruction

You can run the following command to set the timeout time for waiting the ICMP echo packet to **n*100ms** when it check whether the address is distributed.

ip dhcpd ping timeout *n*

Example

You can run the following command to set the timeout time for waiting the ICMP echo packet to **300ms** when it check whether the address is distributed.

ip dhcpd ping timeout 3

4.1.3 ip dhcpd write-time

Parameter

Parameter	Description
time	Interval for the DHCP server to save the address distribution information to the database (unit: minute)

Default

0

Command Mode

Global configuration

Instruction

The following command can be used to set the DHCP server to write the address distribution information to the database every **n** minutes.

ip dhcpd write-time *n*

It is recommended the ip dhcpd write-time is smaller than the default value.

Example

The following example shows that the DHCP server is set to write the address distribution information to the database every two days.

ip dhcpd write-time 1440

4.1.4 ip dhcpd pool

Parameter

Parameter	Description
name	Name of the DHCP address pool

Default

None

Command Mode

Global configuration mode

Instruction

You can run the following command to add the **name** DHCP address pool and enter the DHCP address pool configuration mode.

ip dhcpd pool *name*

Example

The following command in the example is used to add a **test** DHCP address pool and enter the DHCP address pool configuration mode.

ip dhcpd pool test

4.1.5 ip dhcpd enable

Parameter

None

Default

The DHCP service is disabled by default.

Command Mode

Global configuration mode

Instruction

You can run the following command to enable the DHCP service. After the DHCP service is enabled, the DHCP server supports the relay operation; for those address requests that cannot be distributed by themselves, the DHCP requests will be forwarded on the port where the ip-helper-address is configured.

ip dhcpd pool *name*

Example

The following command is used to open the DHCP service.

ip dhcpd enable

4.1.6 ip dhcpd disable

Parameter

None

Default

None

Command Mode

Global configuration

Instruction

Disable DHCP service with following command:

ip dhcpd disable

Example

Disable DHCP service with following command:

ip dhcpd disable

4.2 DHCP Address Pool Configuration Commands

DHCP address pool configuration commands include the following:

- network
- range
- default-router
- dns-server
- domain-name
- lease
- netbios-name-server
- host
- hardware-address
- client-identifier
- client-name

4.2.1 network

network *ip-addr netmask*

Parameter

Parameter	Description

ip-addr	Network address of the address pool for automatic distribution
netmask	Subnet mask

Default

None

Command Mode

DHCP address pool configuration mode

Instruction

You can use the command to configure the network address of the address pool for automatic distribution.

Before the command is configured, make sure that the network number of the IP address for a port on the interface receiving the DHCP packet must be same to the network.

Example

The following example shows how to set the network address of the DHCP address pool to 192.168.20.0 and the subnet mask to 255.255.255.0.

network 192.168.20.0 255.255.255.0

4.2.2 range

range *low-addr high-addr*

Parameter

Parameter	Description
low-addr	Start address of the automatic address distribution range
hogh-addr	End address of the automatic address distribution range

Default

None

Command Mode

DHCP address pool configuration mode

Instruction

You can use the command to configure the automatic address distribution range. You can configure up to eight ranges for each address pool, while each range must be in the network. The command is used only for the automatic distribution mode.

Example

The following example shows how to configure the address distribution range of the DHCP address pool to 192.168.20.210~192.168.20.219.

range 192.168.20.210 192.168.20.219

4.2.3 default-router

default-router *ip-addr*

Parameter

Parameter	Description
ip-addr	Default route which is distributed to the client

Default

None

Command Mode

DHCP address pool configuration mode

Instruction

You can run the command to configure the default route which is distributed to the client; up to four default routes can be configured which are separated through space.

Example

The following example shows how to configure the default route of the DHCP client to 192.168.20.1.

default-router 192.168.20.1

4.2.4 dns-server

dns-server *ip-addr* …

Parameter

Parameter	Description
ip-addr	DNS server address distributed to the client

Default

None

Command Mode

DHCP address pool configuration mode

Instruction

You can run the command to configure the address of the DNS server which is distributed to the client; up to four DNS servers can be configured which are separated through space.

Example

The following example shows how to configure the address of the DNS server distributed to the client to 192.168.1.3.

dns-server 192.168.1.3

4.2.5 domain-name

domain-name *name*

Parameter

Parameter	Description
name	Domain name distributed to the client

Default

None

Command Mode

DHCP address pool configuration mode

Instruction

You can run the command to configure the domain name which is distributed to the client.

Example

The following example shows how to configure the domain name to **test.domain**.

domain-name test.domain

4.2.6 lease

lease {**days** [*hours*][*minutes*] | **infinite**}

Parameter

Parameter	Description
days	Days distributed by the address
hours	Hours distributed by the address
minutes	Minutes distributed by the address
infinite	Means that the addresses will be distributed permanently.

Default

one day

Command Mode

DHCP address pool configuration mode

Instruction

You can run the command to configure the time limitation of the address which is distributed to the client.

Example

The following example shows how to configure the time limitation of the address which is distributed to the client to 12 hours and two days.

Lease 2 12

4.2.7 netbios-name-server

netbios-name-server *ip-addr*

Parameter

Parameter	Description
ip-addr	Address of the netbios name server distributed to the client

Default

None

Command Mode

DHCP address pool configuration mode

Instruction

You can run the command to configure the address of the netbios name server which is distributed to the client; up to four netbios name servers can be configured which are separated through space.

Example

The following example shows how to configure the address of the DNS server distributed to the client to 192.168.1.10.

netbios-name-server 192.168.1.10

4.2.8 host

host *ip-addr netmask*

Parameter

Parameter	Parameter Description
ip-addr	manually distributed ip address of the address pool
netmask	subnet mask

Default

None

Command Mode

DHCP address pool configuration

Instruction

Run the command to configure the manually distributed host ip address of the address pool. The command can only be applied in manually distributed mode. **host** and **range** cannot be configured in the same address pool simultaneously.

Example

The following command is to configure the manually distributed address of DHCP address pool is 192.168.20.200 and the subnet mask is 255.255.255.0.

host 192.168.20.200 255.255.255.0

4.2.9 hardware-address

hardware-address *hardware-address*{ **type**}

Parameter

Parameter	Parameter Description
hardware-address	Hardware address used for matching the client machine.
type	Hardware address type.

Default

The default value of **Type** is 1, which represents Ethernet.

Command Mode

DHCP address pool configuration

Instruction

Run the command to configure the hardware address used for matching the client machine. The address format is two 16 hexadecimal number system, such as ab:cd:ef:gh. The command is only used in the manually distributed mode.

Example

The following command is to configure the hardware address used for matching the client machine: 10:a0:0c:13:64:7d.

hardware-address 10:a0:0c:13:64:7d

4.2.10 client-identifier

ip-bind *ip-addr* **client-identifier** *unique-identifier*

Parameter

Parameter	Description
unique-identifier	Matches the ID of the client.

Default value

None

Command Mode

DHCP address pool configuration mode

Instruction

This command is used to configure the client ID which is used to match the client. The format of the client ID is like **ab.cd.ef.gh**. This command is used only in manual distribution mode.

Example

The following example shows how to set the client ID of the manual-DHCP-distribution address pool to **10:a0:0c:13:64:7d**.

ip-bind *ip-addr* client-identifier 01.10.a0.0c.13.64.7d

4.2.11 client-name

ip-bind *ip-addr* **client-name** *name*

Parameter

Parameter	Description
name	Means the name of the client.

Default value

None

Command Mode

DHCP address pool configuration mode

Instruction

This command is used to configure the host name which is distributed to the client. This command is used only in manual distribution mode.

Example

The following example shows how to set the name of the client to **test**.

ip-bind *ip-addr* client-name test

4.3 DHCP Debugging Commands

DHCP debugging commands include:

- debug ip dhcpd packet
- debug ip dhcpd event

4.3.1 debug ip dhcpd packet

debug ip dhcpd packet

Parameter

None

Default

None

Command Mode

EXEC

Instruction

You can run the command to open the debugging switch of the DHCPD packet.

Example

The following command is used to enable the debugging switch of the DHCPD packet.

debug ip dhcpd packet

4.3.2 debug ip dhcpd event

debug ip dhcpd event

Parameter

None

Default

None

Command Mode

EXEC

Instruction

You can run the command to open the debugging switch of the DHCPD event.

Example

The following command is used to enable the debugging switch of the DHCPD event.

debug ip dhcpd event

DHCPD management commands

DHCP management commands include:

- show ip dhcpd statistic
- show ip dhcpd binding
- clear ip dhcpd statistic
- clear ip dhcpd binding

4.3.3 show ip dhcpd statistic

Parameter

None

Default

None

Command Mode

All modes except the user mode

Instruction

You can run the command to display the DHCPD statistics information, including the number of all types of packets and the number of automatically- or manually-distributed addresses.

Example

The following command is used to display the DHCPD statistics information.

Show ip dhcpd statistic

4.3.4 show ip dhcpd binding

show ip dhcpd binding {*ip-addr*}

Parameter

Parameter	Description
ip-addr	Address whose binding information requires to be displayed

Default

The binding information of all addresses is displayed.

Command Mode

All modes except the user mode

Instruction

You can run the following command to display the binding information, IP address, hardware address, binding type and timeout time about the DHCPD.

Example

The following command is used to display the DHCPD binding information.

Show ip dhcpd binding

4.3.5 show ip dhcpd pool

Parameter

None

Default

None

Command Mode

All modes except the user mode

Instruction

You can run the command to display the information about the DHCPD address pool, including the network number of the address pool, address range, number of the distributed addresses, number of the temporarily-deserted addresses, number of the addresses that can be distributed, manually-distributed IP address and hardware address.

Example

The following command is used to display the statistics information about the DHCPD address pool.

show ip dhcpd pool

4.3.6 clear ip dhcpd statistic

Parameter

None

Default

None

Command Mode

EXEC

Instruction

You can run the command to delete the statistics information about the number of the packets.

Example

The following command is used to delete the statistics information about the number of the packets.

Clear ip dhcpd statistic

4.3.7 clear ip dhcpd binding

clear ip dhcpd binding {*ip-addr*|*}

Parameter

Parameter	Description
ip-addr	Address whose binding information requires to be deleted
*	Deletes all binding information.

Default

The designated address binding information is deleted.

Command Mode

EXEC

Instruction

You can run the command to delete the binding information about the designated address.

Example

The following command is used to delete the binding information about address 192.168.20.210.

clear ip dhcpd binding 192.168.20.210

The following command is used to delete the binding information about address 192.168.20.210 and address 192.168.20.211.

clear ip dhcpd binding 192.168.20.210 192168.20.211

The following command is used to delete all binding information.

clear ip dhcpd binding *

4.3.8 clear ip dhcpd abandoned

Parameter

None

Default

None

Command Mode

EXEC

Instruction

You can run the command to delete the **abandon** identifier.

Example

The following example shows how to delete the **abandon** identifier.

Clear ip dhcpd abandoned

4.4 DHCPD Management Commands

DHCPD management commands include:

- show ip dhcpd statistic
- show ip dhcpd binding
- clear ip dhcpd statistic
- clear ip dhcpd binding

4.4.1 show ip dhcpd statistic

Parameter

None

Default

None

Command Mode

Other modes except the user mode

Instruction

Run the command to show the statistics of DHCPD including numbers of all packets, the address number of automatic distribution and manual distribution.

Example

Run the following command to show statistics of DHCPD.

Show ip dhcpd statistic

4.4.2 show ip dhcpd binding

show ip dhcpd binding {*ip-addr*}

Parameter

Parameter	Parameter Description
ip-addr	Address need to show binding information.

Default

Show the binding information of all addresses.

Command Mode

Other modes except the user mode.

Instruction

Run the command to show DHCPD statistics such as address binding information, IP address, hardware address, binding type and timeout.

Example

Run the following command to show the binding information of DHCPD:

Show ip dhcpd binding

4.4.3 show ip dhcpd pool

Parameter

None

Default

None

Command Mode

Other modes except the user mode

Instruction

Run the command to show DHCPD statistics including the network number of the address pool, the address range, the number of distributed address, the number of abandoned address, the address number to be distributed, manual distributed IP address and hardware address.

Example

Run the following command to show statistics of DHCPD address pool:

show ip dhcpd pool

4.4.4 clear ip dhcpd statistic

Parameter

None

Default

None

Command Mode

Management

Instruction

Run the command to delete statistics about the packet number of DHCPD:

Example

Run following command to delete the statistics of DHCPD packet number:

Clear ip dhcpd statistic

4.4.5 clear ip dhcpd binding

clear ip dhcpd binding {*ip-addr*|*}

Parameter

Parameter	Parameter Description
ip-addr	Address whose binding information requires to be deleted
*	Delete all binding information.

Default

Delete designated address binding information.

Command Mode

Management

Instruction

Run the command to delete the designated address binding information.

Example

Run following command to delete the binding information of 192.168.20.210.

clear ip dhcpd binding 192.168.20.210

Run following command to delete the binding information of 192.168.20.210 and 192.168.20.211.

clear ip dhcpd binding 192.168.20.210 192168.20.211

Run following command to delete all binding information.

clear ip dhcpd binding *

4.4.6 clear ip dhcpd abandoned

Parameter

None

Default

None

Command Mode

Management

Instruction

Run the command to clear the sign of “abandon”.

Example

Run following command to clear the sign of “abandon”.

Clear ip dhcpd abandoned

Chapter 5 DHCP-RELAY SNOOPING Configuration Commands

DHCP-RELAY SNOOPING configuration commands include:

- ip dhcp-relay snooping
- ip dhcp-relay snooping vlan
- ip dhcp-relay snooping database-agent
- ip dhcp-relay snooping db-file
- ip arp inspection vlan
- ip source binding
- arp inspection trust
- dhcp snooping trust
- ip-source trust
- show ip dhcp-relay snooping
- show ip dhcp-relay snooping binding
- debug ip dhcp-relay snooping
- debug ip dhcp-relay event
- debug ip dhcp-relay binding

5.1 dhcp-relay snooping

To enable Dhcp-relay snooping function, run **ip dhcp-relay snooping**; to disable the function, run the negative form of the command.

ip dhcp-relay snooping

no ip dhcp-relay snooping

Parameter

None

Default

Disable dhcp-relay snooping function.

Description

None

Example

Run following command to enable DHCPsnooping function:

```
Switch_config#ip dhcp-relay snooping
Switch_config#
```

5.2 dhcp-relay snooping vlan

ip dhcp-relay snooping vlan *vlan_id*

no ip dhcp-relay snooping vlan *vlan_id*

Parameter

Parameter	Parameter Description
vlan id	VLAN id. The value ranges: 1-4094.

Default

None

Instruction

Configure VLAN of DHCP snooping.

Example

Run following command to snooping DHCP packet on VLAN2.

```
Switch_config#ip dhcp-relay snooping vlan 2
Switch_config#
```

5.3 dhcp-relay snooping vlan vlan_id max-client

Description

ip dhcp-relay snooping vlan *vlan_id* **max-client** *number*

no ip dhcp-relay snooping vlan *vlan_id* **max-client**

Parameter

Parameter	Parameter Description
vlan id	VLAN id. The value ranges: 1-4094.
number	Max user number: 0~65535

Default

Max user number is 65536 by default.

Instruction

Configure available max number of DHCP snooping VLAN. Execute the principle of "First come, first served". That is, new client cannot be distributed if the user number has reached the maximum.

Example

Run following command to snooping DHCP packe ton VLAN2. The max user number is 3.

```
Switch_config#ip dhcp-relay snooping vlan 2 max-client 3
Switch_config#
```

5.4 dhcp snooping trust

Description

dhcp snooping trust

Parameter

None

Default

The default port is non-trust port.

Instruction

No DHCP snooping on DHCP trust port. The negative form of the command is the default value.

Example

Run following command to configure fastEthernet0/1 as DHCP trust port:

Switch_config_f0/1#dhcp snooping trust

5.5 dhcp snooping deny

Description

dhcp snooping deny

Parameter

None

Default

Do not disable snooping detection on the default port.

Instruction

Disable DHCP snooping detection on the port. Enable dhcp snooping trust, ip-source trust and arp inspection trust after configuration. The negative form of the command is the default value.

Example

Run the command to disable fastEthernet0/1 DHCP snooping:

Switch_config_f0/1#dhcp snooping deny

5.6 show ip dhcp-relay snooping

Description

show ip dhcp-relay snooping

Parameter

None

Default

None

Instruction

Show the configuration information of Dhcp-relay snooping.

Example

Run following command to show the configuration information of **dhcp-relay snooping**:

Switch_config#show ip dhcp-relay snooping

5.7 show ip dhcp-relay snooping binding

Description

show ip dhcp-relay snooping binding [all]

Parameter

None

Default

None

Instruction

Show dhcp-relay snooping to the port binding information.

Command all: show all binding information of Dhcp-relay snooping.

Example

Run following command to show binding information of dhcp-relay snooping.

Switch_config#show ip dhcp-relay snooping binding

5.8 debug ip dhcp-relay snooping

Description

debug ip dhcp-relay snooping

no debug ip dhcp-relay snooping

Parameter

None

Default

None

Instruction

Enable/disable Dhcp-relay snooping.

Example

Run following command to enable dhcp-relay snooping.

```
Switch_config#debug ip dhcp-relay snooping
Switch_config#
```

5.9 debug ip dhcp-relay event

Description

debug ip dhcp-relay eventr

no debug ip dhcp-relay event

Parameter

None

Default

None

Instruction

Enable/disable event of Dhcp-relay.

Example

Run following command to enable event of dhcp-relay.

```
Switch_config#debug ip dhcp-relay event
Switch_config#
```

5.10 debug ip dhcp-relay binding

Description

debug ip dhcp-relay binding

no debug ip dhcp-relay binding

Parameter

None

Default

None

Instruction

Enable/disable binding of Dhcp-relay snooping.

Example

Run following command to enable binding of dhcp-relay snooping.

```
Switch_config#debug ip dhcp-relay binding
Switch_config#
```

Chapter 6 **IP Configuration Commands**

6.1 IP Server Configuration Commands

IP server configuration commands include:

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

- show tcp brief
- show tcp statistics
- show tcp tcb

6.1.1 clear tcp

To delete a TCP connection, run the following command:

clear tcp {***local*** *host-name port* **remote** *host-name port* | **tcb** ***address***}

Parameter

Parameter	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

Instruction

The **clear tcp** command is mainly used to delete the terminated TCP connection. Sometimes, because of communication line faults, TCP connection or the peer host is restarted and the TCP connection is actually closed. 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.

```
Router#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
Router#clear tcp local 192.168.20.22 23 remote 192.168.20.120 4420
```

```
Router#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.

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

Related Command

show tcp

show tcp brief

show tcp tcb

6.1.2 clear tcp statistics

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

clear tcp statistics

Parameter

The command has no parameters or keywords.

Command Mode

EXEC

Example

The following example shows how to delete the TCP statistics information:

```
Router#clear tcp statistics
```

Related Command

show tcp statistics

6.1.3 debug arp

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 router 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.

debug arp

no debug arp

Parameter

The command has no parameters or keywords.

Command Mode

EXEC

Example

Router#debug arp

Router#IP ARP: rcvd req src 192.168.20.116 00:90:27:a7:a9:c2, dst 192.168.20.111, Ethernet1/0

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, Ethernet1/1

IP ARP: created an incomplete entry for IP address 192.168.20.77, Ethernet1/0

IP ARP: sent req src 192.168.20.22 08:00:3e:33:33:8a, dst 192.168.20.77, Ethernet1/0

IP ARP: rcvd reply src 192.168.20.77 00:30:80:d5:37:e0, dst 192.168.20.22, Ethernet1/0

The first information line shows that the router receives an ARP request from Ethernet 1/0. 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, Ethernet1/0

The second information line shows that the router receives an ARP address request with IP 192.168.20.139 from interface Etherner 1/1. However, according to the interface configuration of the router, the interface is not in the network claimed by the host. The reason may lie in the incorrect host configuration. If the router 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, Ethernet1/1

The third line shows that, before the router 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 router, the host connects interface Ethernet1/0.

IP ARP: created an incomplete entry for IP address 192.168.20.77, Ethernet1/0

The fourth information shows that the router transmits the ARP request from interface Ethernet 1/0, the IP address of the router 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, Ethernet1/0

The fifth information line shows the router receives the ARP response which is transferred from host 192.168.20.77 to the router'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, Ethernet1/0

6.1.4 debug ip icmp

To display the interaction information of ICMP, run **debug ip icmp**. To close the debugging output, run **no debug ip icmp**.

debug ip icmp

no debug ip icmp

Parameter

The command has no parameters or keywords.

Command Mode

EXEC

Instruction

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

Router#debug ip icmp

Router#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 dst unreachable，including: ---net unreachable ---host unreachable ---protocol unreachable ---port unreachable ---fragmentation needed and DF set ---source route failed ---net unknown ---destination host unknown ---source host isolated ---net prohibited ---host prohibited ---net tos unreachable ---host tos unreachable source quench redirect, including: ---net redirect ---host redirect ---net tos redirect ---host tos redirect echo router advertisement router solicitation time exceeded，including： ---ttl exceeded

	---reassembly timeout parameter problem,including: ---pointer indicating ---option missed ---bad length timestamp timestamp reply information request information reply mask request mask reply If it is the unknown ICMP type, the system will display the ICMP type and its code.
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 48 bytes, 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	Request response packet
from 192.168.20.125	The source address of the ICMP packet is 192.168.20.125.

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	Means the source address of the ICMP packet is 192.168.20.22.
dst 192.168.20.125	Means 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 router cannot route a certain IP packet, the destination-unreachable ICMP packet will be sent to source host 192.168.20.124. The length of the ICMP packet is 36 bytes.

The second information line shows that the router 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.

6.1.5 debug ip packet

To display the IP interaction information, run **debug ip packet**. You can run **no debug ip packet** to stop displaying the IP interaction information.

debug ip packet [**detail**] [*ip-access-list-name*]

no debug ip packet

Parameter

Parameter	Description
detail	(optional) exports the protocol information encapsulated in the IP packet, including protocol number, UDP, number of the TCP port and type of the ICMP packet.
ip-access-list-name	(optional) name of the IP access list for filtering and exporting information Only the information about the IP packet which meets the requirement of the designated IP access list can be exported.
access-group	(optional) name of the IP access list for filtering and exporting information Only the information about the IP packet which meets the requirement of the designated IP access list can be exported.
interface	(optional) name of the port for filtering and exporting information Only the information about the IP packet which meets the requirement of the designated port can be exported.

Command Mode

EXEC

Instruction

The command helps you to know the final direction of each received or locally-generated IP packet flow and detect the reason of communication problems.

The following are potential reasons:

- Forwarded
- Forwarded as the broadcast or 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 router 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

router#debug ip packet

router#IP: s=192.168.20.120 (Ethernet1/0), d=19.0.0.9 (Ethernet1/0), g=192.168.20.1, len=60, redirected

IP: s=192.168.20.22 (local), d=192.168.20.120 (Ethernet1/0), g=192.168.20.120, len=56, sending

IP: s=192.168.20.120 (Ethernet1/0), d=19.0.0.9 (Ethernet1/0), g=192.168.20.1, len=60, forward

IP: s=192.168.20.81 (Ethernet1/0), d=192.168.20.22 (Ethernet1/0), len=56, rcvd

Domain	Description
IP	Means that the information is about the IP packet.
s=192.168.20.120 (Ethernet1/0)	Source address of the IP packet and the name of the interface receiving the packet
d=19.0.0.9 (Ethernet1/0)	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 router 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 becase of ARP resolution failure, the information appears.

The first information line shows that the router 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 Ethernet 1/0; the transmitter interface determined by the routing table is interface Ethernet1/0; 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 Ethernet 1/0 of the router. Hence, the router transmits the ICMP redirect packet.

IP: s=192.168.20.120 (Ethernet1/0), d=19.0.0.9 (Ethernet1/0), 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 addresss of the previous packet, that is, 192.168.20.120. The ICMP redirect packet is transmitted from interface Ethernet1/0 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 (Ethernet1/0), 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 Ethernet1/0; the destination address of the packet is 19.0.0.9. Through the routing table, the packet is found to forward to interface Ethernet1/0; the address of the gateway is 192.168.20.77 and the length of the packet is 60 bytes.

IP: s=192.168.20.120 (Ethernet1/0), d=19.0.0.9 (Ethernet1/0), 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 is Ethernet1/0; the destination address is 192.168.20.22, which is an IP address configured on interface Ethernet1/0 of the router; the length of the packet is 56 bytes.

IP: s=192.168.20.81 (Ethernet1/0), d=192.168.20.22 (Ethernet1/0), len=56, rcvd

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

router#debug ip packet detail

router#IP: s=192.168.12.8 (Ethernet1/0), d=255.255.255.255 (Ethernet1/0), len=328, rcvd, UDP: src=68, dst=67

IP: s=192.168.20.26 (Ethernet1/0), d=224.0.0.5 (Ethernet1/0), len=68, rcvd, proto=89

IP: s=192.168.20.125 (Ethernet1/0), d=192.168.20.22 (Ethernet1/0), len=84, rcvd, ICMP: type=0, code = 0

IP: s=192.168.20.22 (local), d=192.168.20.124 (Ethernet1/0), 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 TCPOther 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 (Ethernet1/0), d=255.255.255.255 (Ethernet1/0), 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 (Ethernet1/0), d=224.0.0.5 (Ethernet1/0), 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 (Ethernet1/0), d=192.168.20.22 (Ethernet1/0), 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 (Ethernet1/0), 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 through the **debug ip packet** command.

Router#**config**

Router_config#**ip access-list standard abc**

Router_config_std_nacl#**permit 192.168.20.125**

Router_config_std_nacl#**exit**

Router_config#**exit**

Router#**debug ip packet abc**

Router#IP: s=192.168.20.125 (Ethernet0/1), d=192.168.20.22 (Ethernet0/1), 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

6.1.6 debug ip raw

To display the information about IP interaction, run **debug ip raw** [**detail**] [***access-list-group***] [***interface***]. To stop displaying information about IP interaction, run **no debug ip raw**.

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

no debug ip raw

Parameter

Parameter	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 type of the TCP packet.
access-group	(optional) name of the IP ACL which is used to filter the output informationOnly 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 informationOnly the information about the IP packets that comply with the designated port can be exported.

Command Mode

EXEC

Instruction

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
- Addressing failed 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 the packet
- 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 router 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

The example is the same to that of the **debug ip packet** command.

Related Command

debug ip tcp packet

6.1.7 debug ip rtp

To display the information about the header compression, run **debug ip rtp** {**header-compression|packets |rtcp**}. You can run **no debug ip rtp** {**header-compression|packets |rtcp**} to stop displaying the information about the header compression.

debug ip rtp {**header-compression|packets |rtcp**}

no debug ip rtp {**header-compression|packets |rtcp**}

Parameter

Parameter	Description
header-compress	RTP/UDP/IP header compression
packets	Packets about data interaction of the RTP/UDP/IP header compression

rtcp	Packets about data interaction of the TCP/IP header compression

Command Mode

EXEC

Instruction

The command helps you to understand the whole process of header compression and interaction.

If you use the command, lots of output information will appear; you had better run the router at a relatively free time, or the system's performance may be badly affected.

Example

router # debug ip rtp header-compress

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: new connection, conn 0,

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7078, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7079, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7080, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7081, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7082, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7083, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7084, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7085, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7086, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4024, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7087, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4025, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4026, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7088, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7089, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4027, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7090, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4028, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7091, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4029, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7092, Gen = 0

2002-1-9 21:36:42

21:32:05: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4030, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7093, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7094, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4032, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7095, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4033, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7096, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4034, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7097, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7098, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4036, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7099, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4037, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7100, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4038, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7101, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: tossing error packet

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7102, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4040, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7103, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4041, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7104, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4042, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7105, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7106, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4044, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7107, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4045, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output uncompressed, conn 0, cksum 0x0000, seq 7108, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: recv COMPRESSED_RTP, conn 0, cksum 0x0000, seq 4046, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7109, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: output COMPRESSED_RTP, conn 0, cksum 0x0000, seq 7110, Gen = 0

2002-1-9 21:36:43

21:32:06: RHC Serial1/0: recv uncompress, conn 0, cksum 0x0000, seq 4048, Gen = 0

no deb all

6.1.8 debug ip tcp packet

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

debug ip tcp packet

no debug ip tcp packet

Parameter

The command has no parameters or keywords.

Command Mode

EXEC

Example

Router#debug ip tcp packet

Router#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	Current state of the TCP connectionFor 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 packet is 192.168.20.125 and the destination port is 3828.
seq 50659460	The sequence number of the packet is 50659460.
DATA 1	Means that the packet contains only one effective byte.
ACK 3130379810	The acknowledgement number of the packet is 3130379810.
PSH	PSH is reset in the control bit of the packet. Other control bits 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 currently
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

6.1.9 debug ip tcp transactions

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

debug ip tcp transactions

no debug ip tcp transactions

Parameter

The command has no parameters or keywords.

Command Mode

EXEC

Example

Router#debug ip tcp transactions

Router#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 TCP interaction information.
rcvd connection attempt to port 23	Receives the connection request from the peer port 23, 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 acknowledgement response and also sending out its connection

	request, and waiting for the connection request acknowledgement 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_1—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) stands 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 (FIN in the control bit of the TCP header is reset).
connection closed	Means that the upper-layer application requires closing the TCP

by user	connection.
connection timed out	Means that the connection is closed because it times out.

Related Command

debug ip tcp packet

6.1.10 debug ip udp

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

debug ip udp

no debug ip udp

Parameter

The command has no parameters or keywords.

Command Mode

EXEC

Example

Router#debug ip udp

Router#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	Means that the packet is received.
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 the message.

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.

6.1.11 ip mask-reply

To enable the router 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

Parameter

The command has no parameters or keywords.

Default

The IP mask request is not answered.

Command Mode

Interface configuration mode

Example

```
!
interface ethernet 1/1
 ip mask-reply
!
```

6.1.12 ip mtu

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

Parameter

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

Default

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

Instruction

If the length of the IP packet exceeds the IP MTU configured on the interface, the router will fragment the packet. Devices on the same physical media can communicate with each other only when they are configured with the same MTU. The MTU value will affect the value of the IP MTU. If the value of IP MTU and that of MTU are same, the value of IP MTU will automatically change to the new value of MTU when the MTU value changes. However, the value of MTU will not change if the value of IP MTU changes.

The minimum value of the IP MTU is 68 bytes, and its maximum value cannot exceed the MTU value configured on the interface.

Example

The following example shows how to set the IP MTU of the interface to 200:

```
!
interface serial0/0
ip mtu 200
!
```

Related Command

mtu

6.1.13 ip redirects

To transmit the IP ICMP redirect packet, run **ip redirects**. To stop transmitting the IP ICMP redirect packet, run **no ip redirects**.

ip redirects

no ip redirects

Parameter

The command has no parameters or keywords.

Default

In general, the IP redirect packet is transmitted by default. However, the function that the IP redirect packet can be transmitted will be automatically disabled if the hot-standby router protocol is configured on the interface. If the configuration of the hot-standby router protocol is cancelled later, the function cannot be automatically enabled.

Command Mode

Interface configuration mode

Instruction

When the router detects that the forwarding interface of the gateway is the same as that of the received packet during the transmission of packets and if the packet-transmitting host directly connects the logic network of the interface, the router can transmit an ICMP redirect packet according to the protocol, notifying the source host of directly taking that router as the gateway for the destination address of the packet without packet forwarding through this router.

If the hot-standby router protocol is configured on an interface, the transmission of IP redirect packet may cause the loss of the packet.

Example

The following example shows how to enable the function of transmitting the ICMP redirect passage on interface ethernet1/0:

```
!
interface ethernet 1/0
 ip redirects
!
```

6.1.14 ip route-cache

To enable the route cache on an interface to forward the IP packet, run **ip route-cache**. To forbid the route cache on an interface, run **no ip route-cache**.

ip route-cache

no ip route-cache

ip route-cache same-interface

no ip route-cache same-interface

Parameter

Parameter	Description

same-interface	Allows the IP packet to be rapidly forwarded from the received interface.

Default

Fast switching is allowed on an interface, while fast switching is forbidden on the same interface.

Command Mode

Interface configuration mode

Instruction

The route cache can conduct the load balance to the forwarded packets based on the source/destination address.

If the route cache is enabled, the packet forwarding rate of the router will be improved. However, the route cache should be forbidden on the low-speed line (64k or even less than 64k).

You can run **ip route-cache same-interface** to allow rapid IP switching on the same interface, that is, the receiver interface is same to the transmitter interface. In general, the function is not recommended to be enabled because the function conflicts with the redirect function of the router. If you has a incompletely-connected network, such as a frame-relay network, you can enable the function on the frame-relay interface. For example, in a frame-relay network consisting of routers A, B and C, there are only links from A to B and from B to C, the communication between router A and router C must be forwarded through router B. In this case, router B receives a packet from router A through a DLCI of an interface, and then transmits the packet to router C through another DLCI of the same interface.

Example

The following command is used to allow fast switching on the same interface.

```
ip route-cache same-interface
```

The following command is used to forbid fast switching even on the same interface.

```
no ip route-cache
```

The following command is used to forbid fast switching only on the same interface.

```
no ip route-cache same-interface
```

The following command is used to enable the default setting (allowing fast switching, the same interface excluded).

```
ip route-cache
```

Related Command

show ip cache

6.1.15 ip source-route

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

ip source-route

no ip source-route

Parameter

The command has no parameters or keywords.

Default

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 router to handle the IP packet with the source IP route option.

ip source-route

Related Command

ping

6.1.16 ip tcp synwait-time

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

ip tcp synwait-time *seconds*

no ip tcp synwait-time

Parameter

Parameter	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

75 seconds

Command Mode

Global configuration mode

Instruction

When the router triggers the TCP connection and if the TCP connection is not established in the designated wait time, the router 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 router, but has relation with the TCP connection of the router itself.

To know the current value, you can run **ip tcp synwait-time?**. The value in the square bracket is the current value.

Example

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

```
Router_config#ip tcp synwait-time 30
Router_config#ip tcp synwait-time ?
<5-300>[30] seconds        -- wait time
```

6.1.17 ip tcp window-size

To set the size of the TCP window, run **ip tcp window-size *bytes***. 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

Parameter

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

Default

2000 bytes

Command Mode

Global configuration mode

Instruction

Do not change the window size at will unless you have a definite purpose. To know the current value, you can run **ip tcp synwait-time ?**. The value in the square bracket is the current value.

Example

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

```
Router_config#ip tcp window-size 6000
Router_config#ip tcp window-size ?
<1-65535>[6000] bytes        -- Window size
```

6.1.18 ip unreachables

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

ip unreachable

no ip unreachable

Parameter

The command has no parameters or keywords.

Default

The ICMP unreachable packet is transmitted.

Command Mode

Interface configuration mode

Instruction

When the router forwards the IP packet, the packet may be dropped because there is no relative route in the routing table. In this case, the router 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 Ethernet 1/0:

```
!
interface ethernet 1/0
 ip unreachables
!
```

6.1.19 ip vrf forwarding

Configure VRF of route interface.

ip vrf forwarding *vrfname*

no ip vrf forwarding *[vrfname]*

Parameter

Parameter	Parameter Description
vrfname	VRF name

Default

Belong to none VRF.

Command Mode

Interface configuration

Instruction

VRF is a prerequisite to configure the command, as the command will delete the ip address configuration under the interface. The command is to configure VRF first and then configure ip address.

Example

The following command is to configure interface g0/0 belongs to VRF“vpn1”:

```
interface g0/0
ip vrf forwarding vpn1
```

6.1.20 show ip cache

To display the route cache which is used for fast IP switching, run **show ip cache [*prefix mask*] [*type number*]**.

show ip cache [*prefix mask*] [*type number*]

Parameter

Parameter	Description
prefix mask	Displays the items whose destination addresses match up the designated prefixes/masks users enter. It is optional.
type number	Displays the items whose transmitter interfaces match up the designated interface types/numbers users enter. It is optional.
rsvp	Displays RSVP-relative items. It is optional.

Command Mode

EXEC

Example

The following example shows that the route cache is displayed:

Router#show ip cache

Source	Destination	Interface	Next Hop
192.168.20.125	2.0.0.124	Serial1/0	2.0.0.124
192.168.20.124	192.168.30.124	Serial1/0	2.0.0.124
2.0.0.124	192.168.20.125	Ethernet1/1	192.168.20.125

Domain	Description
Source	Source address
Destination	Destination address
Interface	Type and number of the transmitted interface
Next Hop	Gateway's address

The following example shows the route cache whose destination address matches up the designated prefix/mask.

Router#show ip cache 192.168.20.0 255.255.255.0

Source	Destination	Interface	Next Hop
2.0.0.124	192.168.20.125	Ethernet0/1	192.168.20.125

The following example shows the route cache whose transmitter interface matches up the designated interface type/mask.

Router#show ip cache s1/0

Source	Destination	Interface	Next Hop
192.168.20.125	2.0.0.124	Serial1/0	2.0.0.124
192.168.20.124	192.168.30.124	Serial1/0	2.0.0.124

6.1.21 show ip irdp

To display the **irdp protocol** information, run **show ip irdp**.

Parameter

The command has no parameters or keywords.

Command Mode

EXEC

Example

```
xuhao_config_e1/0# show ip irdp
Async0/0 ICMP router discovery protocol(IRDP) : OFF

Ethernet1/0 ICMP router discovery protocol(IRDP) : ON
Advertisements occur between every 450 and 600 seconds
Advertisements are sent as broadcasts
Advertisements valid in 1800 seconds
Default preference : 0

Ethernet1/1 ICMP router discovery protocol(IRDP) : OFF

Null0 ICMP router discovery protocol(IRDP) : OFF

Loopback7 ICMP router discovery protocol(IRDP) : OFF

Loopback10 ICMP router discovery protocol(IRDP) : OFF
```

6.1.22 show ip sockets

To display the socket information, run **show ip sockets**.

show ip sockets

Parameter

The command has no parameters or keywords.

Command Mode

EXEC

Example

Router#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	Number of the IP protocol If the value is 17, it means the UDP protocol; if the value is 6, it means the TCP protocol.
Remote	Remote address
Port	Remote port
Local	Local address
Port	Local port
In	Total number of the received bytes
Out	Total number of the transmitted bytes

6.1.23 show ip traffic

To display the flow statistics information, run the following command:

show ip traffic

Parameter

The command has no parameters or keywords.

Command Mode

EXEC

Example

Router#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	Error of the packet's format, such as incorrect IP header length
bad hop count	If the router finds that the TTL value of the packet decreases to zero when it forwards the packet, the packet will be dropped.
no route	Means that the router has no corresponding route.

6.1.24 show tcp

To display the states of all TCP connections, run the following command:

show tcp

Parameter

The command has no parameters or keywords.

Command Mode

EXEC

Example

Router#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---Means that the connection request acknowledgement from the peer is being waited after the local machine receives the peer's connection request, transmits its acknowledgement and also its own connection request. ESTABLISHED---Means that the connection has been established and is now in the data transmission phase in which the upper-layer application can be received or transmitted. FIN_WAIT_1---Means that the peer's acknowledgement and connection termination request is being waited after the local machine transmits the connection termination request to the peer. FIN_WAIT_2---Means that the peer's connection termination request is being waited after the local machine transmits connection termination request to the peer and receives the peer's acknowledgement. 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 to close 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 its connection termination request. CLOSED—Means that there is no connection or the connection has been

	completely 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, 3, 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. 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 acknowledgement 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 acknowledgement 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 acknowledgement 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 acknowledgement 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 handlement
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 acknowledgement 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	Maximum data-segment length allowed by a connection

is	
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

Related Command

show tcp brief

show tcp tcb

6.1.25 show tcp brief

To display the brief information about the TCP connection, run the following command:

show tcp brief [**all**]

Parameter

Parameter	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

Router#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	Internal identifier of the TCP connection
Local Address	Local address and local TCP port
Foreign Address	Remote address and remote TCP port
State	State of the connectionFor details, see the **show tcp** command.

Related Command

show tcp

show tcp tcb

6.1.26 show tcp statistics

To display the statistics data about TCP, run the following command:

show tcp statistics

Parameter

The command has no parameters or keywords.

Command Mode

EXEC

Example

Router#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 router
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 router
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 router
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 acknowledgement

	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

6.1.27 show tcp tcb

To display the state of a TCP connection, run the following command:

show tcp tcb *address*

Parameter

Parameter	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:

Router_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

6.2 ACL Configuration Commands

ACL configuration commands include:

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

6.2.1 deny

To configure the deny rules in IP ACL configuration mode, run **deny *source* [*source-mask*] [log]**; to remote the deny rules from the IP access control list, run **no deny *source* [*source-mask*] [log]**.

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

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

deny src_range source-begin source-end [log]

no deny src_range source-begin source-end [log]

deny *protocol source* *source-mask* ***destination*** *destination-mask* [**precedence** *precedence*] [**tos *tos***] [**log**]

no deny *protocol source* *source-mask* ***destination*** *destination-mask* [**precedence** *precedence*] [**tos** *tos*] [**log**]

deny protocol src_range source-begin source-end dst_range destination-begin destination-end [**precedence** *precedence*] [**tos *tos***] [**log**]

no deny protocol src_range source-begin source-end dst_range destination-begin destination-end [**precedence** *precedence*] [**tos *tos***] [**log**]

The following syntax can also be applied to ICMP:

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

deny icmp src_range source-begin source-end dst_range destination-begin destination-end [***icmp-type***] [**precedence** *precedence*] [**tos *tos***] [**log**]

The following syntax can be used for IGMP:

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

deny igmp src_range source-begin source-end dst_range destination-begin destination-end [***igmp-type***] [**precedence** *precedence*] [**tos *tos***] [**log**]

For TCP, you can use the following syntax:

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

deny tcp src_range source-begin source-end [***src_portrange port-begin port-end***] **dst_range destination-begin destination-end** [***dst_portrange port-begin port-end***] [**established**] [**precedence** *precedence*] [**tos *tos***] [**log**]

For UDP, you can use the following syntax:

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

deny udp src_range source-begin source-end [***src_portrange port-begin port-end***] **dst_range destination-begin destination-end** [***dst_portrange port-begin port-end***] [**precedence** *precedence*] [**tos** ***tos***] [**log**]

Parameter

Parameter	Description
protocol	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 protocol can be further limited, which can be further described.
source	Source network or host numberTwo methods can be used to designate the source: 32-byte binary-system numbers and decimal-system numbers which are separated by four points. The **any** keyword can be the abbreviation of the source and the source's mask of host 0.0.0.0.0.0.0.
source-mask	Mask of the source address The **any** keyword can be the abbreviation of the source and the source's mask of host 0.0.0.0.0.0.0.
destination	Source network or host number, which can designated by the decimal numbers or the binary numbers The **any** keyword can be the abbreviation of the destination and the destination's mask of host 0.0.0.0.0.0.0.
destination-mask	Mask of the destination network The **any** keyword can be the abbreviation of the destination and the destination's mask of host 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.
icmp-type	An optional parameter, which means that the ICMP packet can be filtered based on the type of the ICMP packetThe type of the ICMP packet can be designated by a number between 0 and 255.
igmp-type	An optional parameter, which means that the IGMP packets can be filtered based on the type and name of the IGMP packet The type of the IGMP packet can be designated by a number between 0 and 15.
operator	Compares the source or destination ports. It is an optional parameter. 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	Decimal number or name of the TCP/UDP port, which is optional The port number ranges 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

ARP Access List Configuration

Instruction

You can control the packet transmission on an interface, virtual terminal line access and routing choice update through the access control list. After the match-up is conducted, you shall stop checking the expanded access control list.The segmented IP packet, not the initial segment, will be immediately accepted by any expanded IP access control list. The expanded ACL is used to control the access of the virtual terminal line or limit the content of the routing choice update without matching up the source TCP port, the type of the service value or the packet's priority.

Note:

After an access control list is initially created, any content added later (or entered through the terminal) will be placed 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 that network segment 192.168.5.0 is being forbidden.

```
!
ip access-list standard filter
deny 192.168.5.0 255.255.255.0
!
```

Note:

The IP access control list ends with an implicit deny rule.

Related Command

ip access-group

ip access-list

permit

show ip access-list

6.2.2 ip access-group

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**}.

ip access-group {*access-list-name*}{**in** | **out**}

no ip access-group {*access-list-name*}{**in | out**}

Parameter

Parameter	Description
access-list-name	Name of the access control list, which is a 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

Instruction

The access control list can be used on the incoming or outgoing interface. For the standard incoming access control list, the source address of the packet will be checked according to the access control list after the packet is received. For the expanded access control list, the router will check the destination address. If the access is the address, the software continues to handle the packet. If the access control list forbids the address, the software drops the packet and returns an ICMP unreachable packet.

For the standard access control list, after a packet is received and routed to a control interface, the software checks the source address of the packet according to the access control list. For the expanded access control list, the router will also check the access control list at the receiver terminal. If the access control list at the receiver terminal permits the packet, the software will then forward the packet. If the access control list forbids the address, the software drops the packet and returns an ICMP unreachable packet.

If the designated access control list does not exist, all packets will be allowed.

Example

The following example shows how to apply the **filter** application list on interface Ethernet 0.

```
!
interface ethernet 0
 ip access-group filter out
!
```

Related Command

ip access-list

show ip access-list

6.2.3 ip access-list

To add the IP access control list, run **ip access-list** {**standard | extended**} ***name***.

To delete an IP access control list, run **no ip access-list** {**standard | extended**} ***name***.

ip access-list {**standard | extended**} *name*

no ip access-list {**standard | extended**} *name*

Parameter

Parameter	Description
standard	Specifies the standard access control list.
extended	Specifies the expanded access control list.

name	Name of the access control list, which is a string with up to 20 characters

Default

No IP access control list is defined.

Command Mode

Global configuration mode

Instruction

After the command is run, the system enters the IP access control list mode. You then can run **permit** or **deny** to configure the access rules.

Example

The following example shows that a standard access control list is configured.

```
!
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

6.2.4 permit

To configure the **permit** rules in IP ACL configuration mode, run **permit *source* [*source-mask*] [log]**; to remote the **permit** rules from the IP access control list, run **no permit *source* [*source-mask*] [log]**.

permit *source* [*source-mask***] [log]**

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

permit src_range source-begin source-end [log]

no permit src_range source-begin source-end [log]

permit *protocol source source-mask destination destination-mask* [**precedence** *precedence*] [**tos** *tos*] [**log**]

no permit *protocol source source-mask destination destination-mask* [**precedence** *precedence*] [**tos** *tos*] [**log**]

permit protocol src_range source-begin source-end dst_range destination-begin destination-end [**precedence** *precedence*] [**tos *tos***] [**log**]

no permit protocol src_range source-begin source-end dst_range destination-begin destination-end [**precedence** *precedence*] [**tos *tos***] [**log**]

The following syntax can also be applied to ICMP:

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

permit icmp src_range source-begin source-end dst_range destination-begin destination-end [***icmp-type***] [**precedence** *precedence*] [**tos *tos***] [**log**]

The following syntax can be used for IGMP:

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

permit igmp src_range source-begin source-end dst_range destination-begin destination-end [***igmp-type***] [**precedence** *precedence*] [**tos *tos***] [**log**]

For TCP, you can use the following syntax:

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

permit tcp src_range source-begin source-end [***src_portrange port-begin port-end***] **dst_range destination-begin destination-end** [***dst_portrange port-begin port-end***] [**established**] [**precedence** *precedence*] [**tos *tos***] [**log**]

For UDP, you can use the following syntax:

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

permit udp src_range source-begin source-end [***src_portrange port-begin port-end***] **dst_range destination-begin destination-end** [***dst_portrange port-begin port-end***] [**precedence** *precedence*] [**tos *tos***] [**log**]

Parameter

Parameter	Description
protocol	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 protocol can be further limited, which can be further described.

source	Source network or host number Two methods can be used to designate the source: 32-byte binary-system numbers and decimal-system numbers which are separated by four points. The **any** keyword can be the abbreviation of the source and the source's mask of host 0.0.0.0.0.0.0.0.
source-mask	Mask of the source address The **any** keyword can be the abbreviation of the source and the source's mask of host 0.0.0.0.0.0.0.0.
destination	Source network or host number, which can designated by the decimal numbers or the binary numbers There are two methods to express the destination network or the host's number: the binary system and decimal system The **any** keyword can be the abbreviation of the destination and the destination's mask of host 0.0.0.0.0.0.0.0.
destination-mask	Mask of the destination network The **any** keyword can be the abbreviation of the destination and the destination's mask of host 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 filter at the service layer It is designated by any number between 0 and 15.
icmp-type	An optional packet, which means that the ICMP packet can be filtered based on the type of the ICMP packetThe type of the ICMP packet can be designated by a number between 0 and 255.
igmp-type	An optional parameter, which means that the IGMP packets can be filtered based on the type and name of the IGMP packet The type of the IGMP packet can be designated by a number between 0 and 15.
operator	Compares the source or destination ports. It is an optional parameter. The operations include **lt**, **gt**, **eq** and **neq**. If the operator 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	Decimal number or name of the TCP/UDP port, which is optional The port number ranges between 0 and 65535. The name of the TCP port is listed in the **Usage Guide** 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 access list configuration mode

Instruction

You can control the packet transmission on an interface, virtual terminal line access and routing choice update through the access control list. After the match-up is conducted, you shall stop checking the expanded access control list.

The segmented IP packet, not the initial segment, will be immediately accepted by any expanded IP access control list. The expanded ACL is used to control the access of the virtual terminal line or limit the content of the routing choice update without matching up the source TCP port, the type of the service value or the packet's priority.

Note:

After an access control list is initially created, any content added later (or entered through the terminal) will be placed 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 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 command.

- domain
- snmp
- syslog
- tftp

Example

The following example shows that network segment 192.168.5.0 is allowed.

```
!
ip access-list standard filter
permit 192.168.5.0 255.255.255.0
!
```

Note:

The IP access control list ends with an implicit deny rule.

Related Command

deny

ip access-group

ip access-list

show ip access-list

6.2.5 ip http firewall type

Configure firewall type.

ip http firewalltype type

Parameter

Parameter	Parameter Description
type	Type: 0:IP access list ends with an implicit deny rule; 1:IP access list ends with an implicit permit rule.

Default

The default IP access list ends with an implicit deny rule.

Command Mode

Interface configuration

Instruction

Configure firewall type.

Note: IPACL takes effect only when configured in web interface.

6.2.6 show ip access-list

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

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

Parameter

Parameter	Description
access-list-name	Name of the access control list, which is a string with up to 20 characters

Default

All standard/expanded IP access control lists will be displayed.

Command Mode

EXEC

Instruction

The **show ip access-list** command enables you to specify an access control list.

Example

The following information is displayed after the **show ip access-list** command is run while an access control list is not specified:

```
Router# 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 after you run the **show ip access-list** command with an access control specified:

```
ip access-list extended bbb
permit tcp any any eq www
```

6.2.7 imp access-list

To configure route IP&MAC ACL, run **imp access-list <num>**. To disable the function, run **no imp access-list <num>**.

imp access-list <num>

no imp access-list <num>

Parameter

<1-255>

Default

None

Command Mode

Global Configuration

Instruction

Configure IMP ACL used for matching IP&MAC, for instance, IP address binding and MAC address binding.

Example

The following example shows how to configure IMP ACL:

Router_config#imp access-list 1

6.2.8 permit <ip | any> <mac | any>

To configure permit item of route IP&MAC ACL, run **permit <ip | any> <mac | any>**. To disable the function, run **permit <ip | any> <mac | any>**.

permit <ip | any> <mac | any>

no permit <ip | any> <mac | any>

Parameter

The format of Ip: a.b.c.d, or any (means arbitrary ip address)

The format of Mac: hh:hh:hh:hh:hh:hh or any (means arbitrary MAC address)

Default

None

Command Mode

IMP ACL configuration

Instruction

Configure permit item of IMP ACL.

Example

The following example shows how to configure permit item of IMP ACL.

```
Router_config_imp_acl#permit 1.1.1.1 00:a0:0c:13:64:7d
```

6.2.9 deny <ip | any> <mac | any>

To configure deny item of IP&MAC ACL, run **deny <ip | any> <mac | any>no**. To disable the function, run **deny <ip | any> <mac | any>no**.

deny <ip | any> <mac | any>

no deny <ip | any> <mac | any>

Parameter

The format of Ip: a.b.c.d, or any (means arbitrary ip address)

The format of Mac: hh:hh:hh:hh:hh:hh or any (means arbitrary MAC address)

Default

None

Command Mode

IMP ACL Configuration

Instruction

Configure deny item of IMP ACL.

Example

The following example shows how to configure permit item of IMP ACL:

```
Router_config_imp_acl#deny 1.1.1.2 00:a0:0c:13:64:7d
```

6.2.10 imp access-group

To enable IMP ACL, run **imp access-group <num>**. To disable the function, run **no imp access-group <num>**.

imp access-group <num>

no imp access-group <num>

Parameter

<1-255>

Default

None

Command Mode

Interface configuration

Instruction

Apply IMP ACL to the authentic interface. Ethernet analyzes IP packet and filter by IMP ACL.

Example

The following example shows how to configure IMP ACL:

Router_config_g0/0#imp access-group 1

6.2.11 Ip access-list extended *** massive

Configure the route to adopt with special acl algorithm and accelerate the rate of acl list check.

ip access-list extended * massive**

no ip access-list extended *

Parameter

None

Default

Disable special algorithm.

Command Mode

Global configuration

Instruction

Add keyword “massive” to the common extended access list, that is, deal with the access list with special acl algorithm and accelerate the rate of acl list check.

The algorithm cannot take effect if ip address range and df item have been configured in the access list.

The standard access list does not support the algorithm.

Example

The following example shows how to enable the fast forwarding function:

Router_config#ip access-list extended test massive

Router_config_ext_nacl#permit ip 1.1.1.0 255.255.255.0 2.2.2.0 255.255.255.0

Router_config_ext_nacl#exit

Router_config#

Enable algorithm in Test and localize each rule in Test with the algorithm.

6.3 URPF Configuration Commands

6.3.1 verify ipv4 unicast source reachable-via

Enable URPF function on the interface. URPF has loose URPF and tight URPF. Run the **no verify ipv4 unicast source reachable-via** to disable the function.

verify ipv4 unicast source reachable-via {**any** | **rx**} {allow-default} { access-list-name }

no verify ipv4 unicast source reachable-via {**any** | **rx**} {allow-default} { access-list-name }

Parameter

Parameter	Parameter Description
any	Designate URPF as loose
rx	Designate URPF as strict
allow-default	Indicate whether URPF allows default route
access-list-name	Configure ACL to designate except ion when URPF is failed.

Default

Disable URPF function on all interfaces.

Command Mode

Interface configuration

Instruction

Network administrators can use Unicast Reverse Path Forwarding (Unicast RPF) to help limit the malicious traffic on an enterprise network. This security feature works by enabling a router to verify the reachability of the source address in packets being forwarded. This capability can limit the appearance of spoofed addresses on a network. If the source IP address is not valid, the packet is discarded. Unicast RPF works in one of three different modes: strict mode, loose mode, or VRF mode. **Note** that not all network devices support all three modes of operation.

When administrators use Unicast RPF in strict mode, the packet must be received on the interface that the router would use to forward the return packet. Unicast RPF configured in strict mode may drop legitimate traffic that is received on an interface that was not the router's choice for sending return traffic. Dropping this legitimate traffic could occur when asymmetric routing paths are present in the network.

When administrators use Unicast RPF in loose mode, the source address must appear in the routing table. Administrators can change this behavior using the allow-default option, which allows the use of the default route in the source verification process. Additionally, a packet that contains a source address for which the return route points to the Null 0 interface will be dropped. An access list may also be specified that permits or denies certain source addresses in Unicast RPF loose mode.

Note: URPF shall take effect when enabling verify ipv4 in global configuration mode.

Example

The following example shows how to configure loose URPF on the interface of G0/1 and allow the default route:

```
!
interface GigaEthernet0/1
Ip address 1.1.1.1 255.255.255.0
verify ipv4 unicast source reachable-via any allow-default
!
```

The following example shows how to configure strict URPF on the interface of G0/0:

```
!
interface GigaEthernet0/1
Ip address 1.1.1.1 255.255.255.0
verify ipv4 unicast source reachable-via rx
!
```

6.4 ip fastswitch

To deal with IPv4 forwarding packet in fast switch mode, run **ip fastswitch [***number***]**. To disable the function, run **no ip fastswitch**.

ip fastswitch [*number***]**

no ip fastswitch

Parameter

The length of number system receiving buffer queue: adjust the length to affect the forwarding delay.

Default

Disable fast switch mode.

Command Mode

Global configuration

Instruction

Enable fast switch mode. Some services will be enhanced, for instance: IPv4 forwarding, IPACL and NAT and some services don't change, such as IPSec.

Example

The following example shows how to enable fast switch function and configure system receiving buffer queue as 1024:

```
Router_config#ip fastswitch 1024
```

6.5 FTP Configuration Commands

6.5.1 ftp-server enable

To enable ftp server, run **ftp-server enable** to enable ftp server. To disable the function, run **no ftp-server enable**.

ftp-server enable

no ftp-server enable

Parameter

None

Default

Disable ftp server.

Command Mode

Global configuration

Instruction

Enable ftp server, the router will monitor ftp client in port 21. The router will also monitor ftp over SSL/TLS client in port 990, if ftp-server certificate is configured at the same time.(Refer to 1.6 for more detail.)

Example

The following example shows how to enable ftp server.

Router_config#ftp-server enable

6.5.2 ftp-server maxlogin

To configure the max number of login, run "**ftp-server maxlogin** *maxlogin*". To disable the function, run **no ftp-server maxlogin**.

ftp-server maxlogin *maxlogin*

no ftp-server maxlogin

Parameter

Parameter	Parameter Description
maxlogin	Max number of simultaneous login users, the value range is <1-1024>

Default

No limit to ftp server max login connection

Command Mode

Global configuration

Instruction

Enable ftp server and configure max number of simultaneous login users. When the connected ftp dialogues reach or exceed the number, the system will not accept any other ftp connection.

Example

The following example shows how to configure the max number of simultaneous login users as 5:

```
Router_config#ftp-server maxlogin 5
```

6.5.3 ftp-server attack-defense

To enable ftp server attack defense, run **ftp-server attack-defense**. To disable the function, run "**no ftp-server attack-defense**".

ftp-server attack-defense

no ftp-server attack-defense

Parameter

None

Default

Enable ftp server attack defense.

Command Mode

Global configuration

Instruction

Enable ftp server and configure attack defense. If there appears username or password input error for 5 times within 60 seconds, ftp server will enable the silent mode and no new connection will be accepted in 60s.

The command cannot be used simultaneously with command "ftp-server anonymous-permission".

Example

The following example shows how to enable ftp server attack defense:

```
Router_config#ftp-server attack-defense
```

6.5.4 ftp-server anonymous-permission

To enable ftp server anonymous login, run **ftp-server anonymous-permission**. To resume the default mode, run **no ftp-server anonymous-permission**.

ftp-server anonymous-permission

no ftp-server anonymous-permission

Parameter

None

Default

ftp server does not permit anonymous login.

Command Mode

Global configuration

Instruction

Enable “ftp-server anonymous-permission” and any user can login the ftp server.

The command cannot be used simultaneously with “ftp-server attack-defense”.

Example

The following example shows how to enable ftp server attack defense:

```
Router_config#ftp-server attack-defense
```

6.5.5 ftp-server certificate

To configure the authentication certificate of FTP over SSL/TLS, run **ftp-server certificate *filename***. To disable the function, run no ftp-server certificate.

ftp-server certificate *filename*

no ftp-server certificate

Parameter

Parameter	Parameter Description
filename	Set the filename of FTP over SSL/TLS certificate.

Default

Do not configure the authentication certificate of FTP over SSL/TLS.

Command Mode

Global configuration

Instruction

Configure the authentication certificate of FTP over SSL/TLS. Enable ftp server command if the document is justifiably authenticated. ftp client can login ftps server under port 990 in the mode of FTP over SSL/TLS.

The command cannot verify validity of the document. Reconfigure if there is a prompt “FTP over SSL/TLS socket listen failure”.

Example

The following example shows how to enable the authentication document of FTP over SSL/TLS and ftps:

```
Router_config#ftp-server certificate cert.crt
Router_config#ftp-server enable
```

6.5.6 ftp-server user-group

Configure ftp server user group.

ftp-server user-group *groupname*

no ftp-server user-group *groupname*

Parameter

Parameter	Parameter Description
groupname	Configure FTP user group.

Default

Command Mode

Global configuration

Instruction

The command is to configure user group. It allows the user to add or delete user name and password.

When the user group is deleted, all usernames and passwords will be deleted simultaneously.

Example

The following example is to configure ftp server group:

```
Router_config#ftp-server usergroup grp1
Router_config_ftpd_usergroup#
```

6.5.7 ftp-user

Configure route ftp user group:

ftp-user *username* **password** *password*

no ftp-user *username*

Parameter

Parameter	Parameter Description
username	Configure FTP login username.
password	Configure FTP login password.

Default

Command Mode

ftp server user group configuration

Instruction

The command allows the user to add or delete FTP login user name and password in the mode of ftp server user group configuration.

Example

The following example shows how to configure ftp server usergroup.

Router_config_ftpd_usergroup#ftp-user usr1 password pas1

6.5.8 privilege

To configure the authority of ftp server user group, run **privilege [read | write | execute]**. To resume to the default mode, run **privilege read**.

privilege [read | write | execute]

Parameter

Parameter	Parameter Description
Username	Configure FTP login user name.
password	Configure FTP login password.

Default

Read-only for the user group

Command Mode

ftp server user group configuration

Instruction

Modify the read access and the write access in ftp server user group configuration mode.

Read access: download the file.

Write access: upload the file (There should be no file of the same name in the server. Otherwise, the execute access is needed.)

Execute access: delete file/files; rename file (the files cannot be renamed); create/delete files

Note: The file cannot be named with Chinese.

Example

The following example shows how to configure the accesses of ftp server group including read, write and execute:

```
Router_config_ftpd_usergroup#  privilege read write execute
```

6.6 Attack-Proof Configuration Commands

6.6.1 verify ipv4 enable

Enable or disable attack-proof function.

verify ipv4 enable

no verify ipv4 enable

Parameter

None

Default

Disable attack-proof function.

Command Mode

Global configuration

Instruction

The command is to prevent the host from following attacks including ping flood attack, ping scan attack,syn flood attack, syn port scan attack, fin port scan attack, rst flood attack, udp flood attack, udp port scan attack,ping of death, teardrop attack.

Example

The following example shows how to enable attack-proof function:

!

verify ipv4 enable

6.6.2 verify ipv4 log-enable

Enable or disable attack-proof log alarm function:

verify ipv4 log-enable

no verify ipv4 log-enable

Parameter

None

Default

Disable attack proof log alarm function:

Command Mode

Global configuration

Instruction

The log alarm information will be showed when a host is under attack.

Example

The following example shows how to enable attack-proof log alarm function:

!

verify ipv4 log-enable

6.6.3 verify ipv4 filter

Enable or disable attack-proof packet filtration function:

verify ipv4 filter

no verify ipv4 filter

Parameter

None

Default

Disable attack-proof packet filtration function.

Command Mode

Global configuration

Instruction

Enable attack-proof filtration function and the corresponding packet will be deleted when a host is detected to under attack. For instance, when a host is detected to under the attack of syn flood, the packet over the threshold will be dropped; while when enabling the packet filtration function, all corresponding packets will be dropped when a host is detected to under the attack of syn flood.

Example

The following example shows how to enable attack-proof packet filtration function:

!

verify ipv4 filter

6.6.4 verify ipv4 all

Enable or disable all attack-proof function.

verify ipv4 all

no verify ipv4 all

Parameter

None

Default

Disable all attack-proof function.

Command Mode

Global configuration

Instruction

The command shows how to enable or disable all attack-proof functions.

6.6.5 verify ipv4 icmp

Enable ping flood attack proof and ping scan attack proof.

verify ipv4 icmp {ping-flood| ping-sweep} [*value***]**

no verify ipv4 icmp {ping-flood| ping-sweep} [*value***]**

Parameter

Parameter	Parameter Description
ping-flood	Enable ping flood attack proof
ping-sweep	Enable ping scan attack
value	Configure relevant parameters

Default

Disable ping flood attack proof and pin scan attack proof.

Command Mode

Global configuration

Instruction

The command shows how to configure the threshold of ping flood attack-proof and limit the number of ping packets a host received in one second. The default is 300. The command also configures the time of ping scanning. The default time is 3 seconds. If within 3 seconds ping scans up to 32 different addresses, it will be taken as a ping scan attack.

Example

The following example shows how to enable ping flood attack proof and ping scan attack proof:

```
!
verify ipv4 icmp ping-flood 300
verify ipv4 icmp ping-sweep 3
```

6.6.6 verify ipv4 tcp

Enable following functions including syn flood, syn port scan, fin port scan and rst flood attack.

verify ipv4 tcp {syn-flood| syn-sweep|fin-scan|rst-flood} [*value***]**

no verify ipv4 tcp {syn-flood| syn-sweep|fin-scan|rst-flood} [*value***]**

Parameter

Parameter	Description
syn-flood	Enable syn flood attack proof
syn-sweep	Enable syn port scan attack proof
fin-scan	Enable fin port scan attack proof
rst-flood	Enable rst flood attack proof
value	Configure relevant parameters

Default

Disable corresponding attack-proof functions

Command Mode

Global configuration

Instruction

The command shows how to configure the threshold of syn flood attack-proof and limit the number of syn packets a host received in one second. The default is 300. The command also configures the time of syn scanning. The default time is 3 seconds. If within 3 seconds syn scans up to 32 different addresses, it will be taken as a syn scan attack. The case also applies to fin scan attack-proof and rst flood attack-proof.

Example

The following command shows how to enable syn flood attack-proof, syn port scan attack-proof, fin port scan attack-proof and rst flood attack-proof.

```
!
verify ipv4 tcp syn-flood 300
verify ipv4 tcp syn-sweep 3
verify ipv4 tcp fin-scan 3
verify ipv4 tcp rst-flood 300
```

6.6.7 verify ipv4 udp

Enable udp flood attack-proof and udp port scan attack-proof:

verify ipv4 udp {udp-flood| udp-sweep } [*value***]**

no verify ipv4 udp {udp-flood| udp-sweep } [*value*]

Parameter

Parameter	Description
udp-flood	Enable udp flood attack-proof
udp-sweep	Enable udp port scan attack-proof
value	Configure relevant parameters

Default

Disable relevant attack-proof function

Command Mode

Global configuration

Instruction

The command shows how to configure the threshold of udp flood attack-proof and limit the number of udp packets a host received in one second. The default is 300. The command also configures the time of udp scanning. The default time is 3 seconds. If within 3 seconds udp scans up to 32 different addresses, it will be taken as a udp scan attack.

Example

The following example shows how to enable udp flood attack-proof function and udp scan attack-proof function:

```
!
verify ipv4 udp udp-flood 300
verify ipv4 udp udp-sweep 3
```

6.6.8 verify ipv4 attack

Enable xmas-tree, null-scan, land, smurf, winnuke, ping of death, teardrop, fraggle attack-proof functions:

verify ipv4 attack {xmas-tree|null-scan|land|smurf|winnuke|ping-of-death|teardrop|fraggle} [*value*]

no verify ipv4 attack {xmas-tree|null-scan|land|smurf|winnuke|ping-of-death|teardrop|fraggle} [*value*]

Parameter

Parameter	Description
xmas-tree	Enable xmas-tree attack-proof
null-scan	Enable null scan attack-proof
land	Enable land attack-proof
smurf	Enable smurf attack-proof
winnuke	Enable winnuke attack-proof
ping-of-death	Enable ping of death attack-proof
teardrop	Enable teardrop attack-proof
fraggle	Enable fraggle attack-proof
value	Configure relevant parameters

Default

Disable corresponding attack-proof function

Command Mode

Global configuration

Instruction

The command shows how to configure the time of xmas-tree attack-proof. The default is 3s. If within 3 seconds TCP scanned ports with FIN, PUSH and URG reach 32, it will be taken as a xmas-tree attack.

The command also configures the time of null-scan. The default time is 3 seconds. If within 3 seconds udp scans TCP scanned ports with 0 reach 32, it will be taken as a null-scan attack.

Example

The following example shows how to enable xmas-tree, null-scan, land, smurf, winnuke, ping of death, teardrop, fraggle attack-proof functions:

```
!
verify ipv4 attack Xmas-Tree 3
verify ipv4 attack Null-scan 3
verify ipv4 attack Land
verify ipv4 attack Smurf
verify ipv4 attack WinNuke
verify ipv4 attack Ping-of-Death
verify ipv4 attack TearDrop
verify ipv4 attack Fraggle
```

6.7 Packet Handle Configuration Commands

6.7.1 packet-handle-pause

The command shows how to configure the number of successive handling packets. The handling process pauses per number.

packet-handle-pause per *number*

no packet-handle-pause

Parameter

Parameter	Parameter Description
number	The number of successive handling packets

Default

Default number of successive handling packets is 100.

Command Mode

Global configuration

Instruction

The command shows how to configure the number of successive handling packets. Run “no packet-handle-pause” and the packets are in handling until the waiting handling queue is empty.

Example

The following example shows how to configure the number of successive handling packets:

!

packet-handle-pause per 500

6.8 Hardware Priority Receiving Matching Mode Configuration Commands

6.8.1 pip-watcher

The command shows how to configure packet matching rule, so as to ensure some routing protocol packets are received by the hardware in priority.

pip-watcherarp *match-type match-value*

no pip-watcherarp *match-type match-value*

Parameter

Parameter	Parameter Description
match-type	<0 - 4>, the match type hardware received in priority. 0 means disable the match; 1 means IP protocol segment; 2 means TCP destination port number; 3 means UDP destination port number; 5 means Ethernet protocol segment.
match-value	match-value

Default

None

Command Mode

Global configuration

Instruction

Protocol packets for the route protocol, for instance, BGP, OSPF and ISIS.

Example

The following command ensures ospf packets are received in priority.

pip-watcher 1 0x59

Related command

show cavium pip-watcher