8 IP Service Commands

About This Chapter

8.1 IPv4 Configuration Commands
8.2 ARP Configuration Commands
8.3 DHCP Configuration Commands
8.4 DNS Configuration Commands
8.5 NAT Configuration Commands
8.6 UDP Helper Configuration Commands
8.7 IP Performance Configuration Commands
8.8 Basic IPv6 Configuration Commands
8.9 DHCPv6 Configuration Commands
8.10 IPv6 DNS Configuration Commands
8.11 IPv6 over IPv4 Tunnel Configuration Commands
8.12 IPv4 over IPv6 Tunnel Configuration Commands

8.1 IPv4 Configuration Commands

8.1.1 ip address

Function

The **ip address** command configures an IP address for an interface.

The **undo ip address** command deletes an IP address from an interface.

By default, no IP address is configured for an interface.

 Copyright © Huawei Technologies Co., Ltd.

Format

ip address *ip-address* { *mask* | *mask-length* } [**sub**]

undo ip address [*ip-address* { *mask* | *mask-length* } [**sub**]]

Parameters

Parameter	Description	Value
ip-address { *mask* | *mask-length* }	Specifies the IP address of an interface. • *ip-address* specifies the IP address. • *mask* specifies the mask of the IP address. • *mask-length* specifies the mask length of IP address.	• The value of *ip-address* is in dotted decimal notation. • The value of *mask* is in dotted decimal notation. • The value of *mask-length* is an integer that ranges from 0 to 32.
sub	Configures a secondary IP address for an interface.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **ip address** command configures IP addresses for interfaces on the router so that the router can communicate with different network segments. To connect an interface to multiple network segments, configure multiple IP addresses for the interface. Among these IP addresses, one is the primary IP address and the others are secondary IP addresses. If you configure a new primary IP address for the interface, the new IP address overrides the original one.

- The **undo ip address** command deletes all IP addresses from an interface.
- The **undo ip address** *ip-address* { *mask* | *mask-length* } command deletes the primary IP address of an interface.
- The **undo ip address** *ip-address* { *mask* | *mask-length* } **sub** command deletes a secondary IP address.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

The following conditions are prohibited for different interfaces on the same device:

- The IP addresses are the same.
- The broadcast addresses (with the host number field containing all 1s in the binary mode) corresponding to the IP addresses are the same. For example, if the IP address of interface A is 10.1.1.1/16 and its corresponding broadcast address is 10.1.255.255 and the IP address of interface B is 10.1.1.2/24 and its corresponding broadcast address is 10.1.1.255, the configuration is successful. However, if the IP address of interface B is also 10.1.1.2/16 and its corresponding broadcast address is also 10.1.255.255, the configuration fails.
- The IP address of an interface is the same as the broadcast address of another interface. For example, if the IP address of interface A is 1.1.1.1/28 and its broadcast address is 1.1.1.15 and the IP address of interface B is 1.1.1.15/26, the configuration fails.

You can configure a secondary IP address only after configuring a primary IP address on the interface. You must delete all secondary IP addresses before deleting the primary IP address.

You can configure multiple IP address for a Layer 3 interface on the device, one as the primary IP address, and the others as secondary IP addresses. Each Layer 3 interface can have a maximum of 31 secondary IP addresses.

NOTE

IP addresses of different interfaces on the router cannot be located on the same network segment.

Example

Configure a primary IP address 10.1.0.1 and a secondary IP address 10.2.0.1 for GE1/0/0, with subnet mask 255.255.255.0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.1.0.1 255.255.255.0
[Huawei-GigabitEthernet1/0/0] ip address 10.2.0.1 255.255.255.0 sub
```

Related Topics

5.1.9 display ip interface

8.1.2 ip address unnumbered

Function

The **ip address unnumbered** command configures IP unnumbered on an interface so that the interface can borrow the IP address from another interface.

The **undo ip address unnumbered** command cancels the IP unnumbered configuration on an interface.

By default, an interface does not borrow the IP address from another interface.

Format

ip address unnumbered interface *interface-type interface-number*

 Copyright © Huawei Technologies Co., Ltd.

undo ip address unnumbered

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the numbered interface from which the IP address will be borrowed. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

- You can run the **ip address unnumbered** command to configure certain interfaces, including the ATM interface, dialer interface, tunnel interface, tunnel-template interface, and interface encapsulated with PPP, HDLC, or frame relay to borrow an IP address from an Ethernet interface, loopback interface, or another type of interface. The Ethernet interfaces and Ethernet sub-interfaces only can borrow the IP address from loopback interface.
- Sub-interfaces using FR as the link layer protocol can borrow IP addresses from other interfaces.
- An IP unnumbered interface cannot run dynamic routing protocols because it does not have an IP address itself. To enable the interface to communicate with a peer network segment, configure a static route to the network segment.

When dialer interfaces borrow 32-bit-mask IP addresses from loopback interfaces, pay attention to the following points:

- In automatic dialup mode, after a dialer interface borrows the IP address from a loopback interface, a link is automatically established. No static route needs to be configured.
- In traffic-triggered dialup mode, if a dialer number used to call the remote end is configured using the **dialer number** *dial-number* command, a route to the loopback interface is generated after the dialer interface borrows the IP address of the loopback interface. To enable packets to reach the dialer interface and trigger dialup, configure a static route and specify the dialer interface as the outbound interface.

 Copyright © Huawei Technologies Co., Ltd.

For example, the local dialer interface (dialer1) borrows IP address 1.1.1.1/32 from a loopback interface, the remote IP address is 1.1.1.16, and the destination IP address of dialup packets is 2.1.1.1. To enable traffic to reach dialer1 and trigger dialup, run the **ip route-static 2.1.1.1 255.255.255.255 Dialer1** command to configure a static route and specify dialer1 as the outbound interface.

- In traffic-triggered dialup mode, if the next hop of dialup packets is configured using the **dialer route** *next-hop-address* command, a route to the loopback interface is generated after the dialer interface borrows the IP address of the loopback interface. To trigger dialup, configure a static route, specify the dialer interface as the outbound interface, and specify the next hop.

  For example, the local dialer interface (dialer1) borrows IP address 1.1.1.1/32 from a loopback interface, the remote IP address is 1.1.1.16, and the destination IP address of dialup packets is 2.1.1.1. To enable traffic to reach dialer1 and trigger dialup, run the **ip route-static 2.1.1.1 255.255.255.255 Dialer1 1.1.1.16** command to configure a static route, specify dialer1 as the outbound interface, and specify the next hop.

NOTE

The numbered interface cannot borrow the interface from another interface. Other interfaces cannot borrow the IP address from the unnumbered interface.

The **ip address unnumbered** command can be used only on Layer 3 interfaces.

Example

Configure Tunnel0/0/1 to borrow the IP address from LoopBack0.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] ip address unnumbered interface loopback 0
```

Related Topics

8.1.1 ip address

8.1.3 display ip interface

Function

The **display ip interface** command displays the IP configuration and statistics on interfaces. The statistics include the number of packets and bytes received and sent by interfaces, number of multicast packets sent and received by interfaces, and number of broadcast packets received, sent, forwarded, and discarded by interfaces.

The **display ip interface brief** command displays brief information about interface IP addresses, including the IP address, subnet mask, physical status, link-layer protocol status, and number of interfaces in different states.

Format

display ip interface [*interface-type interface-number*]

 Copyright © Huawei Technologies Co., Ltd.

display ip interface brief [*interface-type* [*interface-number*] | **slot** *slot-id* [**card** *card-number*]]

display ip interface brief [*interface-type*] &<1-8>

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. If no interface is specified, IP configuration and statistics about all interfaces are displayed.	-
brief	Displays brief information, including the IP address, subnet mask, physical status, link-layer protocol status, and number of interfaces in different states.	-
slot *slot-id*	Displays the IP configuration and statistics of interfaces on the specified slot. If the slot number is not specified, brief information related to the IP addresses of the interfaces on all interface boards and main control boards is displayed.	-
card *card-number*	Displays the IP configuration and statistics of interfaces on specified card.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ip interface brief** command to view the following information:

- IP configurations of all interfaces
- IP configurations of interfaces of the specified type and a specified interface
- IP configurations of interfaces that have IP addresses

This command, however, cannot display the IP configurations of Layer 2 interfaces or Eth-Trunk member interfaces.

NOTE

- You can run the **display interface description** command to view the interface description.
- You can run the **display interface** command to view detailed information about the running status and statistics on the interface.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the IP configuration and statistics on GE0/0/0.

```
<Huawei> display ip interface gigabitethernet 0/0/0
GigabitEthernet0/0/0 current state : UP
Line protocol current state : UP
The Maximum Transmit Unit : 1500 bytes
input packets : 1431, bytes : 97912, multicasts : 1426
output packets : 2716, bytes : 179760, multicasts : 2710
Directed-broadcast packets:
 received packets:           0, sent packets:           0
 forwarded packets:          0, dropped packets:        0
ARP packet input number:         11
  Request packet:               11
  Reply packet:                 0
  Unknown packet:               0
Internet Address is 10.5.40.1/24
Broadcast address : 10.5.40.255
TTL being 1 packet number:       0
TTL invalid packet number:       0
ICMP packet input number:        0
  Echo reply:                   0
  Unreachable:                  0
  Source quench:                0
  Routing redirect:             0
  Echo request:                 0
  Router advert:                0
  Router solicit:               0
  Time exceed:                  0
  IP header bad:                0
  Timestamp request:            0
  Timestamp reply:              0
  Information request:          0
  Information reply:            0
  Netmask request:              0
  Netmask reply:                0
  Unknown type:                 0
```

Table 8-1 Description of the **display ip interface** command output

Item	Description
GigabitEthernet1/0/0 current state	Physical status of GigabitEthernet1/0/0: • UP: indicates that the interface is physically Up. • DOWN: indicates that the interface is physically Down. • Administratively DOWN: indicates that the administrator has run the **shutdown** command on the interface.
Line protocol current state	Link layer protocol status of the interface: • UP: The link layer protocol of the interface is running properly. • DOWN: The link layer protocol of the interface is Down or no IP address is configured on the interface.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
The Maximum Transmit Unit	MTU of the interface. The default MTU of an Ethernet interface is 1500 bytes. Packets longer than the MTU are fragmented before being transmitted. If fragmentation is not allowed, the packets are discarded.
input packets : 1431, bytes : 97912, multicasts : 1426	Total number of packets, bytes, and multicast packets received by the interface.
output packets : 2716, bytes : 179760, multicasts : 2710	Total number of packets, bytes, and multicast packets sent by the interface.
Directed-broadcast packets	Number of packets broadcast on the interface directly.
received packets	Total number of received packets.
sent packets	Total number of sent packets.
forwarded packets	Total number of forwarded packets.
dropped packets	Total number of discarded packets.
ARP packet input number	Number of received ARP packets.
Request packet	Number of request packets.
Reply packet	Number of response packets.
Unknown packet	Number of unknown packets.
Internet Address is	IP address and subnet mask of the interface. The displayed information varies according to the IP address allocation mode: • If the IP address is manually configured, the information is displayed as "Internet Address is 10.5.40.1/24." • If the IP address is obtained using DHCP, the information is displayed as "Internet Address is allocated by DHCP, 10.5.40.1/24."
Broadcast address	Broadcast address of an interface.
TTL being 1 packet number	Number of packets with TTL 1.
TTL invalid packet number	Number of packets with invalid TTL.
ICMP packet input number	Number of received ICMP packets.
Echo reply	Number of Echo Reply packets.
Unreachable	Number of Destination Unreachable packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Source quench	Number of Source Quench packets.
Routing redirect	Number of Redirect packets.
Echo request	Number of Echo Request packets.
Router advert	Number of Router Advertisement packets.
Router solicit	Number of Router Solicitation packets.
Time exceed	Number of Time Exceeded packets.
IP header bad	Number of IP header error packets.
Timestamp request	Number of Timestamp Request packets.
Timestamp reply	Number of Timestamp Reply packets.
Information request	Number of Information Request packets.
Information reply	Number of Information Reply packets.
Netmask request	Number of Address Mask Request packets.
Netmask reply	Number of Address Mask Reply packets.
Unknown type	Number of unknown packets.

Display brief IP information about all interfaces.

```
<Huawei> display ip interface brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
The number of interface that is UP in Physical is 2
The number of interface that is DOWN in Physical is 3
The number of interface that is UP in Protocol is 2
The number of interface that is DOWN in Protocol is 3

Interface                   IP Address/Mask      Physical   Protocol
Atm0/0/0                    unassigned           down       down
Bridge-if10                 unassigned           down       down
MFR0/0/1                    unassigned           down       down
NULL0                       unassigned           up         up(s)
Vlanif1                     192.168.200.161/24   up         up
```

Table 8-2 Description of the **display ip interface brief** command output

Item	Description
*down:	Reason why an interface is physically Down. Administratively down indicates that the administrator has run the **shutdown** command on the interface.
^down: standby	Indicates that the interface is a backup interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
(l): loopback	Indicates that the loopback function is enabled on the interface.
(s): spoofing	Indicates that the spoofing function is enabled on the interface.
(E): E-Trunk down	Indicates that the Eth-Trunk is Down because of the protocol negotiation on the E-Trunk.
The number of interface that is UP/DOWN in Physical is	Up or Down state of a physical link and number of interfaces in different states.
The number of interface that is UP/DOWN in Protocol is	Up or Down state of the protocol and number of interfaces in different states.
Interface	Interface type and number.
IP Address/ Mask	IP address and subnet mask of an interface.
Physical	Physical status of an interface: • Up: indicates that the interface is physically Up. (l) indicates that the loopback function is configured on the interface. • Down: indicates that the interface becomes faulty. • *down: indicates that the administrator has run the **shutdown (interface view)** command on the interface. (l) indicates that the loopback function is configured on the interface. • !down: indicates that the FIB module is suspended. In this case, the link protocol status of the interface is Down.
Protocol	Link protocol status of the interface: • Up: indicates that the link protocol of the interface is running properly. (s) indicates that the link protocol status of the interface is Up when this interface is created and has no IP address configured. This is an inherent attribute of an interface. When this interface is configured with an IP address, (s) is still displayed. • Down: indicates that the link protocol of the interface fails or no IP address is configured on the interface. (l) indicates that the loopback function is configured on the interface.

Copyright © Huawei Technologies Co., Ltd.

Related Topics

8.1.4 display interface

8.1.4 display interface

Function

The **display interface** command displays the interface running status and statistics.

Format

display interface [*interface-type* [*interface-number* [.*subinterface-number*] | **main**] | **main**]

display interface slot *slot-id* [**main**]

Parameters

Parameter	Description	Value
interface-type [*interface-number*]	Displays the running status of an interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If the interface type is specified but no interface number is specified, the running status of all the interfaces of this type is displayed.	-
subinterface-number	Displays the running status of a sub-interface.	The value is an integer that ranges from 1 to 4096.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
main	Displays running status and traffic statistics about an interface. • If an interface has no sub-interfaces, status and traffic statistics about the interface are displayed whether you specify the **main** parameter or not. • If an interface has sub-interfaces, status and traffic statistics about the interface and sub-interfaces are displayed if you do not specify the **main** parameter.	-
slot *slot-id*	Specifies the slot ID.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The running status and statistics of an interface includes the physical status, basic configuration, and packet forwarding of the interface. You can use the **display interface** command to collect traffic statistics or locate faults on an interface.

Precautions

If no interface type is specified, the running status and statistics of all the interfaces is displayed. If the interface type is specified but no interface number is specified, the running status of all the interfaces of this type is displayed.

Example

Display the running status, basic configuration, and packet forwarding on Layer 2 Ethernet interface Ethernet2/0/0.

```
<Huawei> display interface ethernet 2/0/0
Ethernet2/0/0 current state : UP
Line protocol current state : UP
```

 Copyright © Huawei Technologies Co., Ltd.

```
Description:HUAWEI, AR Series, Ethernet2/0/0 Interface
Switch Port, PVID :    1, TPID : 8100(Hex), The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0018-2000-0083
Last physical up time   : 2010-07-21 15:35:37
Last physical down time : 2010-07-20 01:06:25
Current system time: 2010-07-21 16:07:53-05:13
Port Mode: COMMON COPPER
Speed :  100,  Loopback: NONE
Duplex: FULL,  Negotiation: ENABLE
Mdi   : AUTO,  Clock   : -
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 0 bits/sec,Record time: -
Output peak rate 0 bits/sec,Record time: -

Input:  126 packets, 34204 bytes
  Unicast:              0,  Multicast:             52
  Broadcast:           74,  Jumbo:                  0
  Discard:              0,  Total Error:            0

  CRC:                  0,  Giants:                 0
  Jabbers:              0,  Throttles:              0
  Runts:                0,  Symbols:                0
  Ignoreds:             0,  Frames:                 0

Output:  2398 packets, 799486 bytes
  Unicast:              0,  Multicast:          1461
  Broadcast:         1477,  Jumbo:                 0
  Discard:              0,  Total Error:           53

  Collisions:          32,  ExcessiveCollisions:    21
  Late Collisions:      0,  Deferreds:              0

    Input bandwidth utilization threshold : 100.00%
    Output bandwidth utilization threshold: 100.00%
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
```

Table 8-3 Description of the **display interface** command output

Item	Description
current state	Current interface status: • DOWN: indicates that the interface is disabled. • UP: indicates that the interface is enabled.
Line protocol current state	Link layer protocol status of the interface: • DOWN: indicates that the link layer protocol of the interface fails or no IP address is assigned to the interface. • UP: indicates that the link layer protocol of the interface is running properly.
Description	Interface description. To configure the description for an interface, run the **description** command.
PVID	Default VLAN ID of the interface.
The Maximum Frame Length	Maximum frame length allowed by the interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
IP Sending Frames' Format	Format of the frame contained in the sent IP packet, which can be PKTFMT_ETHNT_2, Ethernet_802.3, or Ethernet_SNAP.
Hardware address	MAC address of the device.
Last physical up time	Last time the interface goes Up physically. If this field displays "-", the physical status of the interface does not change.
Last physical down time	Last time the interface goes Down physically. If this field displays "-", the physical status of the interface does not change.
Current system time	Current system time. If the time zone is configured and the daylight saving time is used, the time is in YYYY/MM/DD HH: MM: SS UTC±HH: MM DST format.
Port Mode	Working mode of the common interface: • COMMON COPPER: The interface is an electrical interface. • COMMON FIBER: The interface is an optical interface. Run **combo-port**. The working mode of the combo interface is configured. • AUTO: The combo interface automatically select the working mode. • AUTO FIBER: The combo interface automatically select optical working mode. • AUTO COPPER: The combo interface automatically select electrical working mode. • FORCE FIBER: The combo interface is configured as an optical interface. • FORCE COPPER: The combo interface is configured as an electrical interface.
Speed	Current rate of the interface. • In auto-negotiation mode, the **auto speed** command configures the rate of an interface. • In non-auto negotiation mode, the **speed** command configures the rate of an interface.
Loopback	Loopback configuration of the interface. The **loopback** command configures loopback on an interface.
Duplex	Duplex mode of the interface.
Negotiation	Auto-negotiation mode of the interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Mdi	Network cable type of the interface.
Clock	Clock mode of the combo interface.
Last 300 seconds input rate	Incoming packet rate (bits per second and packets per second) within the last 300 seconds.
Last 300 seconds output rate	Outgoing packet rate (bits per second and packets per second) within the last 300 seconds.
Input peak rate	Maximum incoming packet rate.
Output peak rate	Maximum outgoing packet rate.
Input	Total number of received packets.
Output	Total number of sent packets.
Unicast	Number of unicast packets received or sent by the interface.
Multicast	Number of multicast packets received or sent by the interface.
Broadcast	Number of broadcast packets received or sent by the interface.
Jumbo	Number of jumbo frames received or sent by the interface.
Discard	Number of packets discarded by the interface during physical layer detection. These packets are discarded because the interface is congested. The device does not support the **Discard** field for Layer 2 Ethernet interfaces.
Total Error	Number of error packets found during physical layer detection.
CRC	Number of CRC error packets received by the interface.
Giants	Number of jumbo frames with correct Frame Check Sequence (FCS) received by the interface. **NOTE** For the AR109, AR109W, AR109GW-L, AR121, AR121W, AR121GW-L, AR129, AR129W, AR129CVW, AR129CV, AR129GW-L, AR129CGVW-L, AR161, AR161W, AR161EW, AR161EW-M1, AR161G-L, AR161G-Lc, AR161G-U, AR169, AR169W, AR169EW, AR169CVW, AR169EGW-L, AR169CVW-4B4S, AR169G-L, AR169-P-M9, AR169W-P-M9, AR169RW-P-M9, this item indicates the number of received packets with length exceeding the maximum jumbo frame size.
Jabbers	Number of jumbo frames with incorrect FCS received by the interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Throttles	Number of undersized frames with incorrect FCS received by the interface. Undersized frames are the frames that are shorter than 64 bytes and have the correct format and valid CRC field.
Runts	Number of undersized frames with correct FCS values received by the interface. Undersized frames are the frames that are shorter than 64 bytes and have the correct format and valid CRC field.
Symbols	Number of received frames with coding errors.
Ignoreds	Number of received MAC control frames with OpCode not being PAUSE.
Frames	Number of packets with incorrect 802.3 length.
Collisions	Number of frames that the interface stops sending when conflicts are detected during transmission.
ExcessiveCollisions	Number of frames that experience more than 16 consecutive conflict events and fail to be sent.
Late Collisions	Number of frames that experience conflict events and are delayed. The first 512 bits of these frames have been sent but these frames are delay because conflicts are detected.
Deferreds	Number of packets delayed because conflicts are detected before transmission.
Input bandwidth utilization threshold	Threshold for inbound bandwidth usage.
Output bandwidth utilization threshold	Threshold for outbound bandwidth usage.
Input bandwidth utilization	Inbound bandwidth usage. This parameter is not collected on interfaces that do not support statistics collection, and the value is fixed at 0% or --.
Output bandwidth utilization	Outbound bandwidth usage. This parameter is not collected on interfaces that do not support statistics collection, and the value is fixed at 0% or --.

Display the running status, basic configuration, and packet forwarding on Layer 3 Ethernet interface Ethernet2/0/0.

```
<Huawei> display interface ethernet 2/0/0
Ethernet2/0/0 current state : UP
Line protocol current state : UP
Description:HUAWEI, AR Series, Ethernet2/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 192.168.4.2/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0018-2000-0083
```

 Copyright © Huawei Technologies Co., Ltd.

```
Last physical up time   : 2010-09-08 15:35:37
Last physical down time : 2010-09-08 01:06:25
Current system time: 2010-10-21 16:07:53
Port Mode: COMMON COPPER
Speed :  100,  Loopback: NONE
Duplex: FULL,  Negotiation: ENABLE
Mdi   : AUTO,  Clock   : -
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 0 bits/sec,Record time: -
Output peak rate 0 bits/sec,Record time: -

Input:  126 packets, 34204 bytes
  Unicast:              0,  Multicast:             52
  Broadcast:           74,  Jumbo:                  0
  Discard:              0,  Total Error:            0

  CRC:                  0,  Giants:                 0
  Jabbers:              0,  Throttles:              0
  Runs:                 0,  Symbols:                0
  Ignoreds:             0,  Frames:                 0

Output:  2398 packets, 799486 bytes
  Unicast:              0,  Multicast:          1461
  Broadcast:         1477,  Jumbo:                 0
  Discard:              0,  Total Error:           53

  Collisions:          32,  ExcessiveCollisions:    21
  Late Collisions:      0,  Deferreds:              0

    Input bandwidth utilization threshold : 100.00%
    Output bandwidth utilization threshold: 100.00%
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
```

Table 8-4 Description of the **display interface** command output

Item	Description
current state	Current interface status: • DOWN: indicates that the interface is disabled. • UP: indicates that the interface is enabled.
Line protocol current state	Link layer protocol status of the interface: • DOWN: indicates that the link layer protocol of the interface fails or no IP address is assigned to the interface. • UP: indicates that the link layer protocol of the interface is running properly.
Description	Interface description. To configure the description for an interface, run the **description** command.
The Maximum Transmit Unit is	MTU of the interface. For example, the default MTU of an Ethernet interface is 1500 bytes. Packets whose size is greater than the MTU are fragmented before being transmitted. If fragmentation is not allowed, the packets are discarded.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Internet Address is	IP address and mask length of the interface. The displayed information varies according to the IP address allocation mode: • If the IP address is manually configured, the information is displayed as "Internet Address is 192.168.4.2/24." • If the IP address is obtained using DHCP, the information is displayed as "Internet Address is allocated by DHCP, 192.168.4.2/24."
IP Sending Frames' Format	Format of the frame contained in the sent IP packet, which can be PKTFMT_ETHNT_2, Ethernet_802.3, or Ethernet_SNAP.
Hardware address	MAC address of the device.
Last physical up time	Last time the interface goes Up physically. If this field displays "-", the physical status of the interface does not change.
Last physical down time	Last time the interface goes Down physically. If this field displays "-", the physical status of the interface does not change.
Current system time	Current system time. If the time zone is configured and the daylight saving time is used, the time is in YYYY/MM/DD HH: MM: SS UTC±HH: MM DST format.
Port Mode	Working mode of the interface: • COMMON COPPER: The interface works as an electrical interface. • COMMON FIBER: The interface works as an optical interface. If the interface is a combo interface: • COMBO AUTO: The combo interface automatically selects the working mode. • FORCE FIBER: The combo interface is configured as an optical interface. • FORCE COPPER: The combo interface is configured as an electrical interface. To configure the working mode for an interface, run the **combo-port** command.
Speed	Current rate of the interface. • In auto-negotiation mode, the **auto speed** command configures the rate of an interface. • In non-auto negotiation mode, the **speed** command configures the rate of an interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Loopback	Loopback configuration of the interface. To configure loopback on an interface, run the **loopback** command.
Duplex	Duplex mode of the interface.
Negotiation	Auto-negotiation mode of the interface.
Mdi	Network cable type of the interface.
Clock	Clock mode of the combo interface.
Last 300 seconds input rate	Incoming packet rate (bits per second and packets per second) within the last 300 seconds.
Last 300 seconds output rate	Outgoing packet rate (bits per second and packets per second) within the last 300 seconds.
Input peak rate	Maximum incoming packet rate.
Output peak rate	Maximum outgoing packet rate.
Input	Total number of received packets.
Output	Total number of sent packets.
Unicast	Number of unicast packets received or sent by the interface.
Multicast	Number of multicast packets received or sent by the interface.
Broadcast	Number of broadcast packets received or sent by the interface.
Jumbo	Number of jumbo frames received or sent by the interface. If the value is -, the number of jumbo frames cannot be collected on the device. **NOTE** Only interfaces of AR2220 MPUs support this statistical item.
Discard	Number of packets discarded by the interface during physical layer detection. These packets are discarded because the interface is congested. **NOTE** Only Layer 3 Ethernet interfaces of AR201, AR1220 and AR2220 MPUs support this statistical item.
Total Error	Number of error packets found during physical layer detection.
CRC	Number of CRC error packets received by the interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Giants	Number of jumbo frames with correct FCS received by the interface. **NOTE** For the AR109, AR109W, AR109GW-L, AR121, AR121W, AR121GW-L, AR129, AR129W, AR129CVW, AR129CV, AR129GW-L, AR129CGVW-L, AR161, AR161W, AR161EW, AR161EW-M1, AR161G-L, AR161G-Lc, AR161G-U, AR169, AR169W, AR169EW, AR169CVW, AR169EGW-L, AR169CVW-4B4S, AR169G-L, AR169-P-M9, AR169W-P-M9, AR169RW-P-M9, this item indicates the number of received packets with length exceeding the maximum jumbo frame size.
Jabbers	Number of jumbo frames with incorrect FCS received by the interface.
Throttles	Number of undersized frames with incorrect FCS received by the interface. Undersized frames are the frames that are shorter than 64 bytes and have the correct format and valid CRC field.
Runts	Number of undersized frames with correct FCS values received by the interface. Undersized frames are the frames that are shorter than 64 bytes and have the correct format and valid CRC field.
Symbols	Number of received frames with coding errors.
Ignoreds	Number of received MAC control frames with OpCode not being PAUSE.
Frames	Number of packets with incorrect 802.3 length.
Collisions	Number of frames that the interface stops sending when conflicts are detected during transmission.
ExcessiveCollisions	Number of frames that experience more than 16 consecutive conflict events and fail to be sent.
Late Collisions	Number of frames that experience conflict events and are delayed. The first 512 bits of these frames have been sent but these frames are delay because conflicts are detected.
Deferreds	Number of packets delayed because conflicts are detected before transmission.
Input bandwidth utilization threshold	Threshold for inbound bandwidth usage.
Output bandwidth utilization threshold	Threshold for outbound bandwidth usage.
Input bandwidth utilization	Inbound bandwidth usage. This parameter is not collected on interfaces that do not support statistics collection, and the value is fixed at 0% or --.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Output bandwidth utilization	Outbound bandwidth usage. This parameter is not collected on interfaces that do not support statistics collection, and the value is fixed at 0% or --.

Display the packet forwarding on dialer1 interface.

```
<Huawei> display interface dialer 1
Dialer1 current state : UP
Line protocol current state : UP (spoofing)
Description:HUAWEI, AR Series, Dialer1 Interface
Route Port,The Maximum Transmit Unit is 1500, Hold timer is 0(sec)
Internet protocol processing : disabled
Link layer protocol is PPP
LCP initial
Physical is Dialer
Current system time: 2017-12-08 23:02:15
    Input: 8837 packets, 851857 bytes
    Output: 0 packets, 0 bytes
Last 600 seconds input rate 11358 bits/sec, 14 packets/sec
Last 600 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 65350 bits/sec,Record time: 2017-12-06 04:16:23
Output peak rate 0 bits/sec,Record time: -


ipv4
    Input: 8837 packets, 851857 bytes
    Output: 0 packets, 0 bytes
Last 600 seconds input rate 0 bits/sec, 0 packets/sec
Last 600 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 65350 bits/sec,Record time: 2017-12-06 04:16:23
Output peak rate 0 bits/sec,Record time: -


ipv6
    Input: 0 packets, 0 bytes
    Output: 0 packets, 0 bytes
Last 600 seconds input rate 30744573456171227 bits/sec, 30744573456182571 packet
s/sec
Last 600 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 0 bits/sec,Record time: -
Output peak rate 0 bits/sec,Record time: -

    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
```

Table 8-5 Description of the **display interface** command output

Item	Description
current state	Current interface status: • DOWN: indicates that the interface is disabled. • UP: indicates that the interface is enabled.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Line protocol current state	Link layer protocol status of the interface. • DOWN: indicates that the link layer protocol of the interface fails or no IP address is assigned to the interface. • UP: indicates that the link layer protocol of the interface is running properly.
Description	Interface description. To configure the description for an interface, run the **description** command.
The Maximum Transmit Unit is	MTU of the interface. For example, the default MTU of an Ethernet interface is 1500 bytes. Packets whose size is greater than the MTU are fragmented before being transmitted. If fragmentation is not allowed, the packets are discarded.
Internet Address is	IP address and mask length of the interface. The displayed information varies according to the IP address allocation mode: • For a statically configured IP address: Internet Address is 192.168.4.2/24 If the IP address is statically configured, the information is displayed as "Internet Address is 192.168.4.2/24". • If the IP address is obtained using DHCP, the information is displayed as "Internet Address is allocated by DHCP, 192.168.4.2/24".
IP Sending Frames' Format	Format of frames sent by the IP protocol, including PKTFMT_ETHNT_2, Ethernet_802.3, and Ethernet_SNAP.
Hardware address	MAC address of the device.
Input	Total number of received packets.
Output	Total number of sent packets.
Last 600 seconds input rate	Incoming packet rate (bits per second and packets per second) within the last 600 seconds.
Last 600 seconds output rate	Outgoing packet rate (bits per second and packets per second) within the last 600 seconds.
Input peak rate	Maximum incoming packet rate.
Output peak rate	Maximum outgoing packet rate.
ipv4	Number of IPv4 packets.
ipv6	Number of IPv6 packets.
Input bandwidth utilization	Inbound bandwidth usage. This parameter is not collected on interfaces that do not support statistics collection, and the value is fixed at 0% or --.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Output bandwidth utilization	Outbound bandwidth usage. This parameter is not collected on interfaces that do not support statistics collection, and the value is fixed at 0% or --.

Related Topics

5.1.2 description (interface view)

5.1.16 shutdown (interface view)

8.2 ARP Configuration Commands

8.2.1 arp detect-mode unicast

Function

The **arp detect-mode unicast** command configures an interface to send ARP aging probe packets in unicast mode.

The **undo arp detect-mode unicast** command restores the default configuration of detection modes on an interface.

By default, an interface sends the last ARP aging probe packet in broadcast mode, and the rest ARP aging probe packets are sent in unicast mode.

Format

arp detect-mode unicast

undo arp detect-mode unicast

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before an ARP entry is aged, the interface periodically sends ARP aging probe packets at a set interval to update ARP entries. The device deletes an ARP entry if

 Copyright © Huawei Technologies Co., Ltd.

it does not receive a reply after a specified number of probes. The aging probe packet can be a unicast or broadcast packet.

When a non-Huawei device connected to a Huawei router receives an ARP aging probe packet whose destination MAC address is a broadcast address, the non-Huawei device checks the ARP table. If the mapping between the IP address and the MAC address of the Huawei router exists in the ARP table, the non-Huawei device discards the ARP aging probe packet. Then the Huawei router cannot receive a response and deletes the corresponding ARP entry. As a result, traffic from the non-Huawei device cannot be forwarded. Therefore, when a non-Huawei device is connected to a Huawei router, configure the Huawei switch to send ARP aging probe packets in unicast mode. The non-Huawei device needs to respond to the ARP aging probe packet.

Precautions

If the IP address of the peer device remains the same but the MAC address changes frequently, it is recommended that you configure ARP aging probe packets to be broadcast.

When the MAC address of the peer device remains the same, and the bandwidth of the network is insufficient, it is recommended that you set the interface to send ARP aging probe packets in unicast mode.

Example

Configure an interface to send ARP aging probe packets in unicast mode.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] arp detect-mode unicast
```

Related Topics

8.2.2 arp detect-times

8.2.3 arp expire-time

8.2.2 arp detect-times

Function

The **arp detect-times** command sets the number of ARP probes for aging dynamic ARP entries.

The **undo arp detect-times** command restores the default number of ARP probes for aging dynamic ARP entries.

By default, the number of ARP probes for aging dynamic ARP entries is 3.

Format

arp detect-times *detect-times*

undo arp detect-times

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
detect-times	Specifies the number of ARP probes for aging dynamic ARP entries.	The value is an integer ranging from 0 to 10. The default value is 3.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **arp detect-times** command sets the number of ARP probes for aging dynamic ARP entries to reduce address resolution errors. Before aging a dynamic ARP entry, the system first performs probes. If no response is received after the number of probes reaches the upper limit, the ARP entry is deleted.

Precautions

If the number of ARP probes is set to 0, the system directly deletes expired ARP entries.

Example

Set the number of ARP probes to 5 on Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] arp detect-times 5
```

Related Topics

8.2.3 arp expire-time

8.2.1 arp detect-mode unicast

8.2.3 arp expire-time

Function

The **arp expire-time** command sets the aging time of dynamic ARP entries.

The **undo arp expire-time** command restores the default aging time of dynamic ARP entries.

By default, the aging time of dynamic ARP entries is 1200 seconds, that is, 20 minutes.

Copyright © Huawei Technologies Co., Ltd.

Format

arp expire-time *expire-time*

undo arp expire-time

Parameters

Parameter	Description	Value
expire-time	Specifies the aging time of dynamic ARP entries.	The value is an integer ranging from 60 to 62640, in seconds. The default value is 1200 seconds, that is, 20 minutes.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **arp expire-time** command sets the aging time of dynamic ARP entries to reduce address resolution errors.

Precautions

After proxy ARP is enabled, the aging time of ARP entries on hosts should be shortened so that invalid ARP entries can be deleted as soon as possible. Then IP packet forwarding failures decrease on the router.

The command can be configured globally or on the specified interface. If the command is not configured on the interface, the aging expiry time of a dynamic ARP entry will be the one configured globally. If the command is both configured globally and on the specified interface, the aging expiry time of a dynamic ARP entry will be the one configured on the interface.

Example

Set the aging time of dynamic ARP entries to 600s on Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] arp expire-time 600
```

Related Topics

8.2.2 arp detect-times

8.2.1 arp detect-mode unicast

 Copyright © Huawei Technologies Co., Ltd.

8.2.4 arp learning multicast enable (system view)

Function

The **arp learning multicast enable** command globally enables a device to learn multicast MAC addresses and generate dynamic ARP entries.

The **undo arp learning multicast enable** command globally disables a device from learning multicast MAC addresses and generate dynamic ARP entries.

By default, a device is globally disabled from learning multicast MAC addresses.

Format

arp learning multicast enable

undo arp learning multicast enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A MAC address corresponding to an IP address may be a multicast MAC address. In this case, a network administrator has to configure a static ARP entry. A device can generate dynamic ARP entries if enabled to learn multicast MAC addresses. This way reduces a network administrator's workload of configuring static ARP entries and reduces network operation and maintenance costs.

Precautions

After a device is enabled to learn multicast MAC addresses, the device may be attacked by ARP attack packets carrying multicast MAC addresses as source MAC addresses.

Example

Globally enable a device to learn multicast MAC addresses and generate dynamic ARP entries.

```
<Huawei> system-view
[Huawei] arp learning multicast enable
```

 Copyright © Huawei Technologies Co., Ltd.

8.2.5 arp-ping ip

Function

The **arp-ping ip** command checks whether an IP address on a LAN is in use by sending ARP packets.

Format

arp-ping ip *ip-address* [**timeout** *time-out-value*] [**interface** *interface-type interface-number* [**vlan-id** *vlan-id*]]

Parameters

Parameter	Description	Value
ip-address	Specifies the destination IP address.	The value is in dotted decimal notation.
interface *interface-type interface-number*	Specifies the type and number of the interface that sends ARP packets. Where, • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. You must configure an outbound interface through which ARP packets are sent if you monitor the local IP address.	By default, you can search the FIB table for an outbound interface through which ARP packets are sent if you monitor a non-local IP address.
timeout *time-out-value*	Specifies the timeout period for an ARP-ping test. You are advised to specify the parameter if you monitor the local IP address.	The value is an integer in the range 1 to 10, in seconds. The default value is 3s.
vlan-id *vlan-id*	Specifies the ID of a VLAN.	The ID is an integer ranging from 1 to 4094. If this parameter is not specified, the VLAN ID is considered as 0. When the specified outbound interface is a Layer 2 interface, you need to configure *vlan-id*; when the specified outbound interface is a Layer 3 interface, you cannot configure *vlan-id*.

Views

All views

Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **arp-ping ip** command checks whether an IP address on a LAN is in use by sending ARP packets.

The **ping** command can also check whether an IP address is in use. If the destination host or the router configured with the firewall function are configured not to reply to ping packets, there is no response to the ping packet. Consequently, the IP address is considered unused. ARP is a Layer 2 protocol; therefore, ARP packets can pass through the firewall that is configured not to reply to ping packets. In this way, the preceding situation does not occur.

In addition, the length of an ARP Request packet is smaller than that of an Internet Control Message Protocol (ICMP) packet used in the **ping** command, occupying fewer network resources. You are advised to use the **arp-ping ip** command.

Precautions

ARP has been enabled and the device can send and receive ARP packets.

If the IP address specified in the **arp-ping ip** command is the IP address of the local device or a loopback address, the detection fails.

Example

Run the **arp-ping ip** command to check whether the IP address 10.1.1.1 is used.

```
<Huawei> arp-ping ip 10.1.1.1
ARP-Pinging 10.1.1.1:

10.1.1.1 is used by 00e0-fc91-8d70
```

Related Topics

8.2.6 arp-ping mac

8.2.6 arp-ping mac

Function

The **arp-ping mac** command checks whether a MAC address is used by another device on a LAN by sending ICMP packets or checks the IP address corresponding to the MAC address.

Format

arp-ping mac *mac-address* { *ip-address* [**vpn-instance** *vpn-instance-name*] | **interface** *interface-type interface-number* }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
mac-address	Specifies the destination MAC address.	The value is in the H-H-H format. Each H contains one to four hexadecimal numbers, such as 00e0 and fc01. If you enter fewer than four digits, 0s are padded before the input digits. For example, if e0 is entered, 00e0 is displayed. The MAC address cannot be a multicast, broadcast, or virtual MAC address.
ip-address	Specifies the network segment to be queried.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance.
interface *interface-type interface-number*	Specifies the type and number of the interface that sends and receives ICMP packets. Where, • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you know a specific MAC address but not the corresponding IP address on a network segment, you can run the **arp-ping mac** command to send ICMP packets.

ICMP has been enabled and the device can send and receive ICMP packets.

Example

Run the **arp-ping mac** command on VLANIF2 to check whether the MAC address 00e0-fca6-a45d is used on a LAN.

```
<Huawei> arp-ping mac 00e0-fca6-a45d interface vlanif 2
 OutInterface: VLANIF2 MAC[00-E0-FC-A6-A4-5D], press CTRL_C to break
```

 Copyright © Huawei Technologies Co., Ltd.

```
----- ARP-Ping MAC statistics -----
1 packet(s) transmitted
1 packet(s) received

IP ADDRESS              MAC ADDRESS
192.168.1.122           00-E0-FC-A6-A4-5D
```

Table 8-6 Description of the arp-ping mac command output

Item	Description
IP ADDRESS	IP address mapping the specified MAC address.
MAC ADDRESS	MAC address to be checked.

Related Topics

8.2.5 arp-ping ip

8.2.7 arp-proxy enable

Function

The **arp-proxy enable** command enables routed proxy ARP on an interface.

The **undo arp-proxy enable** command disables routed proxy ARP on an interface.

By default, routed proxy ARP is disabled on an interface.

Format

arp-proxy enable

undo arp-proxy enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If two hosts on different physical networks of the same logical network segment are not configured with the default gateways, you can use the **arp-proxy enable**

Copyright © Huawei Technologies Co., Ltd.

command to enable routed proxy ARP on a device between the two hosts to resolve IP addresses of the hosts.

Precautions

Routed ARP proxy allows hosts on different physical networks of the same logical network segment to communicate. The IP addresses of the hosts on a subnet have the same network ID; therefore, the default gateway address does not need to be configured on the hosts.

Example

Enable routed proxy ARP on Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] arp-proxy enable
```

Related Topics

8.2.8 arp-proxy inner-sub-vlan-proxy enable

8.2.9 arp-proxy inter-sub-vlan-proxy enable

8.2.8 arp-proxy inner-sub-vlan-proxy enable

Function

The **arp-proxy inner-sub-vlan-proxy enable** command enables intra-VLAN proxy ARP.

The **undo arp-proxy inner-sub-vlan-proxy enable** command disables intra-VLAN proxy ARP.

By default, intra-VLAN proxy ARP is disabled.

Format

arp-proxy inner-sub-vlan-proxy enable

undo arp-proxy inner-sub-vlan-proxy enable

Parameters

None

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

If host isolation is configured on the router, you need to configure intra-VLAN proxy ARP to allow hosts to communicate in a VLAN.

Precautions

QinQ sub-interfaces, Dot1q sub-interfaces, QinQ Stacking sub-interfaces and QinQ Mapping sub-interfaces do not support proxy ARP within a VLAN.

Example

Enable intra-VLAN proxy ARP on VLANIF 10.

```
<Huawei> system-view
[Huawei] interface vlanif 10
[Huawei-Vlanif10] arp-proxy inner-sub-vlan-proxy enable
```

Related Topics

8.2.7 arp-proxy enable

8.2.9 arp-proxy inter-sub-vlan-proxy enable

8.2.9 arp-proxy inter-sub-vlan-proxy enable

Function

The **arp-proxy inter-sub-vlan-proxy enable** command enables inter-VLAN proxy ARP or proxy ARP on termination sub-interfaces.

The **undo arp-proxy inter-sub-vlan-proxy enable** command disables inter-VLAN proxy ARP or proxy ARP on termination sub-interfaces.

By default, inter-VLAN proxy ARP or proxy ARP on termination sub-interfaces is disabled.

Format

arp-proxy inter-sub-vlan-proxy enable

undo arp-proxy inter-sub-vlan-proxy enable

Parameters

None

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

To implement communication between different VLANs, you must enable inter-VLAN proxy ARP on the interface.

In a super-VLAN, hosts of different sub-VLANs cannot communicate. To implement communication between them, you must enable inter-VLAN proxy ARP on the VLANIF interface of the super-VLAN.

Precautions

After inter-VLAN proxy ARP is enabled and packets are sent from different VLANs but do not have the corresponding ARP entries, ARP packets are replicated in all VLANs on the involved sub-interface. If a lot of VLANs are configured, a large number of ARP packets need to be replicated, causing heavy burden on the peer device and abnormalities (such as high CPU usage and broadcast suppression) on downstream devices. In addition, the local device may fail to send ARP packets in time due to the replication of a large number of packets, which may lead to ARP learning failures. Therefore, do not configure too many VLANs on an interface.

Example

Enable inter-VLAN proxy ARP on VLANIF 10.

```
<Huawei> system-view
[Huawei] interface vlanif 10
[Huawei-Vlanif10] arp-proxy inter-sub-vlan-proxy enable
```

Related Topics

8.2.7 arp-proxy enable

8.2.8 arp-proxy inner-sub-vlan-proxy enable

8.2.10 arp regularly-refresh enable

Function

The **arp regularly-refresh enable** command enables the scheduled ARP refresh function.

The **undo arp regularly-refresh enable** command disables the scheduled ARP refresh function.

By default, the scheduled ARP refresh function is enabled.

Format

arp regularly-refresh enable

undo arp regularly-refresh enable

Parameters

None

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

By default, the scheduled ARP refresh function is enabled on the device, and the device updates ARP entries every 10 hours.

Example

Disable the scheduled ARP refresh function.

```
<Huawei> system-view
[Huawei] undo arp regularly-refresh enable
```

8.2.11 arp send-packet

Function

The **arp send-packet** command configures the ARP unicast detection function.

Format

arp send-packet *ip-address mac-address* **interface** *interface-type interface-number* [**vid** *vid* [**cevid** *cevid*]]

Parameters

Parameter	Description	Value
ip-address	Specifies a destination IP address for a unicast ARP request packet to be sent.	This value is in dotted decimal notation.
mac-address	Specifies a destination MAC address for a unicast ARP request packet to be sent.	The value is in H-H-H format. H is a hexadecimal number of 1 to 4 digits. *mac-address* cannot be FFFF-FFFF-FFFF.
interface *interface-type interface-number*	Specifies the type and number of an interface for sending out a unicast ARP request packet.	-
vid *vid*	Specifies an outer tag value for a unicast ARP request packet to be sent.	The value is an integer ranging from 1 to 4094.
cevid *cevid*	Specifies an inner tag value for a unicast ARP request packet to be sent.	The value is an integer ranging from 1 to 4094.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check whether a peer device is reachable, run the **arp send-packet** command to configure a local interface to send a unicast ARP request packet that carries the peer device's IP and MAC addresses as the destination addresses.

- If the peer is reachable, the peer sends an ARP reply packet to the local device. Then, the local device uses information carried in the ARP reply packet to create or update an ARP entry for the peer.
- If the peer is unreachable, the peer device does not send an ARP reply packet. The local device does not generate an ARP entry.

The ARP entries learned or updated by the local device will be deleted after their aging time expires and can be updated again after the local device receives ARP request packets from the peer device.

Example

Configure GE1/0/0 to send a unicast ARP request packet that carries the destination IP address 2.2.2.3 and destination MAC address 5489-98f4-786e.

```
<Huawei> arp send-packet 2.2.2.3 5489-98f4-786e interface gigabitethernet 1/0/0
```

8.2.12 arp static

Function

The **arp static** command configures static ARP entries.

The **undo arp static** command deletes static ARP entries.

By default, the ARP mapping table is empty and address mappings are obtained using dynamic ARP.

Format

arp static *ip-address mac-address* [**vpn-instance** *vpn-instance-name*]

arp static *ip-address mac-address* **vid** *vlan-id* [**cevid** *ce-vid*] **interface** *interface-type interface-number*

undo arp static *ip-address* [*mac-address*] [**vpn-instance** *vpn-instance-name* | **vid** *vlan-id* [**cevid** *ce-vid*] **interface** *interface-type interface-number*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address in a static ARP entry.	The value is in dotted decimal notation.
mac-address	Specifies the MAC address of a static ARP entry.	The value is in H-H-H format. An H contains one to four hexadecimal numbers.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance. The parameter is used for the MPLS VPN feature. When this parameter is set, it indicates that the ARP entry is of the VPN instance. **NOTE** After the name of a VPN instance is specified, the device can automatically learn the outbound interface, with no need for specifying it.	The value must be an existing VPN instance.
interface *interface-type interface-number*	Specifies the outbound interface of a static ARP packet. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. **NOTE** If the IP address corresponding to the specified ARP entry belongs to the VPN, an outbound interface cannot be specified.	-
vid *vlan-id*	Specifies the ID of the VLAN to which a static ARP entry belongs.	The value is an integer ranging from 1 to 4094.
cevid *ce-vid*	Specifies the inner VLAN ID.	The value is a decimal integer ranging from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure security and facilitate management, you may need to configure mappings between IP addresses and MAC addresses. In this case, run the **arp**

 Copyright © Huawei Technologies Co., Ltd.

static command to configure a fixed ARP mapping entry that maps an IP address to a MAC address.

A static ARP entry cannot be dynamically modified.

A static ARP entry is used in the following situations:

- Direct the packets whose destination IP addresses are not on the local network segment to a gateway on the local network segment so that the packets can be forwarded by the gateway.
- Bind the destination IP addresses of invalid packets to a nonexistent MAC address so that the invalid packets are filtered out.

Precautions

If a static ARP entry to be created exists, the system updates the entry.

After a static ARP entry is configured, it cannot be dynamically updated.

The IP address specified by *ip-address* and the IP address of the outbound interface specified by **interface** must be on the same network segment.

- For Layer 3 physical interfaces and Layer 3 Eth-Trunk interfaces, run the **arp static** *ip-address mac-address* command to configure static ARPentries.
- For VLANIF interfaces and Dot1q termination sub-interfaces, run the **arp static** *ip-address mac-address* **vid** *vlan-id* **interface** *interface-type interface-number* command to configure static ARP entries.
- For QinQ termination sub-interfaces, run the **arp static** *ip-address mac-address* **vid** *vlan-id* **cevid** *ce-vid* **interface** *interface-type interface-number* command to configure static ARP mapping entries with double tags. *vid* specified in this command must be the same as *pe-vid* in the **qinq termination pe-vid ce-vid** command, and *ce-vid* must be within the value range of *ce-vid* in the **qinq termination pe-vid ce-vid** command.
- For interfaces bound to a VPN instance:
  - For Layer 3 physical interfaces and Layer 3 Eth-Trunk interfaces, run the **arp static** *ip-address mac-address* **vpn-instance** *vpn-instance-name* command to configure static ARP entries.
  - For VLANIF interfaces and Dot1q termination sub-interfaces, run the **arp static** *ip-address mac-address* **vid** *vlan-id* **interface** *interface-type interface-number* command to configure static ARP entries.
  - For QinQ termination sub-interfaces, run the **arp static** *ip-address mac-address* **vid** *vlan-id* **cevid** *ce-vid* **interface** *interface-type interface-number* command to configure static ARP mapping entries with double tags. *vid* specified in this command must be the same as *pe-vid* in the **qinq termination pe-vid ce-vid** command, and *ce-vid* must be within the value range of *ce-vid* in the **qinq termination pe-vid ce-vid** command.

Example

Configure a static ARP entry that maps the IP address 10.0.0.1 to the MAC address aaaa-fccc-1212.

```
<Huawei> system-view
[Huawei] arp static 10.0.0.1 aaaa-fccc-1212
```

 Copyright © Huawei Technologies Co., Ltd.

Configure a static ARP entry that maps the IP address 10.1.1.1 to MAC address 0efc-0505-86e3. This entry belongs to VLAN 10. The outbound interface is Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] arp static 10.1.1.1 0efc-0505-86e3 vid 10 interface ethernet 2/0/0
```

Configure a static ARP entry that maps the IP address 10.1.1.1 to MAC address 0efc-0505-86e3. This ARP entry belongs to the VPN instance **vpn1**.

```
<Huawei> system-view
[Huawei] ip vpn-instance vpn1
[Huawei-vpn-instance-vpn1] ipv4-family
[Huawei-vpn-instance-vpn1-af-ipv4] quit
[Huawei-vpn-instance-vpn1] quit
[Huawei] arp static 10.1.1.1 0efc-0505-86e3 vpn-instance vpn1
```

Configure an ARP entry that maps the IP address 10.1.1.1 to the MAC address 00e0-fc01-0000. The VLAN ID in the outer VLAN tag is 10 and the VLAN ID in the inner VLAN tag is 100. The outbound interface is GE1/0/0.1.

```
<Huawei> system-view
[Huawei] arp static 10.1.1.1 00e0-fc01-0000 vid 10 cevid 100 interface gigabitethernet 1/0/0.1
```

Related Topics

8.2.16 display arp interface

8.2.31 reset arp

8.2.13 arp-suppress enable

Function

Using the **arp-suppress enable** command, you can enable ARP suppression.

Using the **undo arp-suppress** command, you can disable ARP suppression.

By default, ARP suppression is disabled but is enabled on VLANIF interfaces.

Format

arp-suppress enable

undo arp-suppress

Parameters

None

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

If the system receives a great number of ARP packets from the same source at a time, it needs to update ARP entries repeatedly, causing performance deterioration. To ensure system performance, you can enable ARP suppression. The system then only responds to ARP Request packets but does not update ARP entries.

If ARP suppression is enabled for all interfaces, ARP entries on some interfaces cannot be updated temporarily. ARP suppression is applicable to only VLANIF and Eth-Trunk interfaces. By default, it always takes effect on VLANIF interfaces. It can be configured on other logical interfaces.

After the **undo arp-suppress** command is executed, ARP suppression is enabled only on VLANIF interfaces.

Example

Enable ARP suppression.

```
<Huawei> system-view
[Huawei] arp-suppress enable
```

8.2.14 display arp

Function

The **display arp** command displays all ARP mapping entries.

Format

display arp [**all** | **brief**]

Parameters

Parameter	Description	Value
all	Displays all ARP mapping entries.	-
brief	Displays brief information about ARP mapping entries.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

This command displays all ARP mapping entries, including the aging time of ARP entries, ARP entry type, and VPN instance to which ARP entries belong.

NOTE

If Layer 3 VXLAN is configured on the device, you can query dynamic ARP entries through BDIF interfaces, but not through physical interfaces.

If Layer 3 VXLAN is configured on the device, you cannot query static ARP entries through physical and BDIF interfaces.

Example

Display all ARP mapping entries.

```
<Huawei> display arp all
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                VLAN/CEVLAN(SIP/DIP)      PVC
--------------------------------------------------------------------------------
192.168.0.1     00e0-fc01-0000            S--
192.168.118.1   0018-2000-0083            I -         Vlanif11
10.1.1.1        0018-2000-0083            I -         Vlanif10
10.1.1.116      0018-2000-0083            I -         GE2/0/0
10.1.1.118      0001-0c01-3401  14        D-0         GE2/0/0
10.1.1.4        0016-ecb7-a879  18        D-0         GE2/0/0
192.168.10.1    0018-8267-7f7d            D-0         GE1/0/4
                                      10/-
192.168.10.1    0018-8267-7f7d            S--         vbdif10
                                    1.1.1.1/2.2.2.2
192.168.10.1    0018-8267-7f7d            D-0         vbdif10
                                    1.1.1.1/2.2.2.3
--------------------------------------------------------------------------------
Total:9         Dynamic:4       Static:1     Interface:6
```

Display brief information about all ARP mapping entries.

```
<Huawei> display arp brief
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE  INTERFACE
                                VLAN/CEVLAN(SIP/DIP)      PVC
--------------------------------------------------------------------------------
192.168.200.176 5489-9876-2c5c            I -   Eth1/0/0
192.168.200.100 5489-98f4-5a8e 18         D-0   Eth1/0/1
10.1.1.2        5489-9876-2c5e            I -   Eth1/0/2
192.168.10.1    0018-8267-7f7d            S--   vbdif10
                                    1.1.1.1/2.2.2.2
--------------------------------------------------------------------------------
Total:4         Dynamic:1       Static:0     Interface:3
```

Table 8-7 Description of the display arp command output

Item	Description
IP ADDRESS	IP address in the ARP entry.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
MAC ADDRESS	MAC address in the ARP entry. If the field is Incomplete, the entry is a fake ARP entry. If a large number of ARP Miss messages are sent to the upper-layer software, the system resources will be exhausted in processing the ARP Miss messages. To resolve this problem, the system automatically generates ARP fake entries instead of ARP entries. You can run the **arp-fake expire-time** command to configure the aging time of fake ARP entries.
EXPIRE(M)	Remaining lifetime of ARP entries, in minutes.
TYPE	ARP entry type and slot ID of the LPU that obtains the entry. The entry type contains 3 bits. The first bit can be any of the following: • I: Interface, indicating the MAC address of the interface • D: Dynamic, indicating the dynamic entry obtained through the ARP packet • S: Static, indicating the static entry obtained through static configuration If the second bit is F, the ARP entry has been reported to the routing module, the route to this IP address has been calculated, and the entry in the FIB has been updated. **NOTE** If the entry is not reported to the routing module, this field displays "-". For the ARP entry with the type as "I", this flag bit does not exist. The third bit indicates the slot ID of the LPU that obtains the entry. **NOTE** For the ARP entry with the type as "I" or "S", this field displays "-".
VPN-INSTANCE	Name of the VPN instance to which the ARP entry belongs. The value is set using the **ip vpn-instance** command.
INTERFACE	Type and number of the interface that has learnt ARP entries.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
VLAN/CEVLAN	ID of the VLAN to which the ARP entry belongs. The value is set using the **vlan** command.
SIP/DIP	Source IP address and destination IP address of a VXLAN tunnel.
PVC	Interface where the PVC exists and the corresponding VPI/VCI.
Total	Total number of ARP entries in the ARP mapping table.
Dynamic	Number of dynamic ARP entries in the ARP mapping table.
Static	Number of static ARP entries in the ARP mapping table.
Interface	Number of ARP entries in the ARP mapping table on the local interface.

Related Topics

8.2.12 arp static
8.2.18 display arp dynamic
8.2.16 display arp interface
8.2.20 display arp network
8.2.22 display arp static
8.2.23 display arp statistics
8.2.31 reset arp

8.2.15 display arp error packet

Function

The **display arp error packet** command displays the latest ten ARP error packets.

Format

display arp error packet

Parameters

None

Views

All views

Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

If a device cannot learn ARP entries, you can run this command to check the latest received ARP error packets. The ARP error packets help locate the fault.

Example

Display the latest ten ARP error packets.

```
<Huawei> display arp error packet
-------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:34:53]:
00 01 08 00 06 04 00 01 00 25 9E 4B 1F 75 0A 8A
4E 02 00 00 00 00 00 00 0A 8A 4E FF 00 00 00 00
00 00 00 00 00 00 FF FF FF FF FF FF 00 25
-------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:34:54]:
00 01 08 00 06 04 00 01 00 13 72 FD E7 1C 0A 8A
4E 98 00 00 00 00 00 00 0A 8A 4E 30 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
-------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:34:55]:
00 01 08 00 06 04 00 01 00 13 72 9B 21 A7 0A 8A
4E 82 00 00 00 00 00 00 0A 8A 4E 01 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
-------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:35:05]:
00 01 08 00 06 04 00 01 00 13 72 9B 21 A7 0A 8A
4E 82 00 00 00 00 00 00 0A 8A 4E 01 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
-------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:35:05]:
00 01 08 00 06 04 00 01 00 E0 FC 8F B2 DD 0A 8A
4E 01 00 00 00 00 00 00 0A 8A 4F FA 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
-------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:35:08]:
00 01 08 00 06 04 00 01 00 0F E2 5C 8C EA AC 12
3E FE 00 00 00 00 00 00 AC 12 3E FE 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
-------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:35:11]:
00 01 08 00 06 04 00 01 00 1B B9 78 25 2E 0A 8A
4E A5 00 00 00 00 00 00 0A 8A 4E 2D 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
-------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:35:15]:
00 01 08 00 06 04 00 01 00 13 72 9B 21 A7 0A 8A
4E 82 00 00 00 00 00 00 0A 8A 4E 01 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
-------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:35:19]:
00 01 08 00 06 04 00 01 00 13 72 9B 21 A7 0A 8A
4E 82 00 00 00 00 00 00 0A 8A 4E 01 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
-------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:35:22]:
00 01 08 00 06 04 00 01 00 E0 FC 8F B2 DD 0A 8A
4E 01 00 00 00 00 00 00 0A 8A 4F FA 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

 Copyright © Huawei Technologies Co., Ltd.

Table 8-8 Description of the display arp error packet command output

Item	Description
interface	Interface name.
time	Time when an ARP error packet is received.

Related Topics

8.2.16 display arp interface

8.2.31 reset arp

8.2.16 display arp interface

Function

The **display arp interface** command displays ARP mapping entries of a specified interface.

Format

display arp interface *interface-type interface-number* [**vid** *vlan-id* [**cevid** *cevlan-id*]]

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-
vid *vlan-id*	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
cevid *cevlan-id*	Specifies the CE VLAN ID.	The value is an integer ranging from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To monitor dynamic ARP entries or locate the faults in ARP, you can run this command to check the ARP entries.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display all the ARP entries of Ethernet2/0/0.

```
<Huawei> display arp interface ethernet 2/0/0
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE       INTERFACE   VPN-INSTANCE
                                VLAN/CEVLAN PVC
--------------------------------------------------------------------------------
192.168.1.11    0000-0a41-0201            I -        Ethernet1/0/1       r1
192.168.1.1     0000-0a41-0200  15        D-6        Ethernet1/0/1       r1
--------------------------------------------------------------------------------
Total:2         Dynamic:1       Static:0    Interface:1
```

Table 8-9 Description of the display arp interface command output

Item	Description
IP ADDRESS	IP address in the ARP entry.
MAC ADDRESS	MAC address in the ARP entry. If the field is Incomplete, the entry is a fake ARP entry. If a large number of ARP Miss messages are sent to the upper-layer software, the system resources will be exhausted in processing the ARP Miss messages. To resolve this problem, the system automatically generates ARP fake entries instead of ARP entries. You can run the **arp-fake expire-time** command to configure the aging time of fake ARP entries.
EXPIRE(M)	Remaining lifetime of the ARP entry, in minutes.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
TYPE	ARP entry type and slot ID of the LPU that obtains the entry. The entry type contains 3 bits. The first bit can be any of the following: • I: Interface, indicating the MAC address of the interface • D: Dynamic, indicating the dynamic entry obtained through the ARP packet • S: Static, indicating the static entry obtained through static configuration The second bit can only be F, indicating that the entry is reported to the routing module, the route to this IP address is calculated, and entries in the FIB are correspondingly updated. **NOTE** If the entry is not reported to the routing module, this field displays "-". For the ARP entry with the type as "I", this flag bit does not exist. The third bit indicates the slot ID of the LPU that obtains the entry. **NOTE** For the ARP entry with the type as "I" or "S", this field displays "-".
INTERFACE	Type and number of the interface that has learnt ARP entries.
VPN-INSTANCE	Name of the VPN instance to which the ARP entry belongs. The value is set using the **ip vpn-instance** command.
VLAN/CEVLAN	ID of the VLAN to which the ARP entry belongs. The value is set using the **vlan** command.
PVC	Interface where the PVC exists and the corresponding VPI/VCI.
Total	Number of ARP entries.
Dynamic	Number of dynamic ARP entries.
Static	Number of static ARP entries.
Interface	Number of ARP entries of the local interface.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

8.2.12 arp static

8.2.31 reset arp

6.3.43 vlan

8.2.17 display arp ip-conflict track

Function

The **display arp ip-conflict track** command displays recorded information about the detected IP address conflict.

Format

display arp ip-conflict track

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Route flapping caused by IP address conflicts affects user services. To help users quickly locate IP conflicts to better manage IP addresses of network devices, run the **display arp ip-conflict track** command to view the recorded information about the detected IP address conflict.

NOTE

The maximum number of IP conflict information that can be recorded by the system is 200, and the oldest recorded information will be covered by newly added if the conflicted IP address is more than 200.

Example

Display the information of the detected IP address conflict.

```
<Huawei> display arp ip-conflict track
  Conflict type       : Remote IP Conflict
  IP address          : 10.1.1.1
  System time         : 2011-04-10 06:59:43
  Conflict count      : 1
  Suppress count      : 0
  Old interface       : GE1/0/1
  Receive interface   : GE1/0/2
```

 Copyright © Huawei Technologies Co., Ltd.

```
Old VLAN/CEVLAN     : 100/0
Receive VLAN/CEVLAN : 100/0
Old MAC             : 00e0-ca63-8141
Receive MAC         : 00e0-ca63-8142
```

Table 8-10 Description of the display arp ip-conflict track command output

Item	Description
Conflict type	IP address conflict type
IP address	Conflicting IP address
System time	System time when an IP conflict occurred
Conflict count	Total number of the IP conflict times **NOTE** The field is displayed as 0 if the ARP entry corresponding to the IP address expires or is deleted.
Suppress count	Number of the suppressed IP conflicts **NOTE** The field is displayed as 0 if the ARP entry corresponding to the IP address expires or is deleted.
Old interface	Interface recorded in the ARP entry of the IP address
Receive interface	Interface that receives the ARP packet with duplicate IP address
Old VLAN/CEVLAN	VLAN and CEVLAN recorded in the ARP entry of the IP address
Receive VLAN/CEVLAN	VLAN and CEVLAN configured on the interface that receives the ARP packet with duplicate IP address
Old MAC	Source MAC address recorded in the ARP entry of the IP address
Receive MAC	Source MAC address of the second ARP packet with duplicate IP address

8.2.18 display arp dynamic

Function

The **display arp dynamic** command displays all dynamic ARP entries.

Format

display arp dynamic

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display all dynamic ARP mapping entries.

```
<Huawei> display arp dynamic
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                          VLAN/CEVLAN
--------------------------------------------------------------------------------
10.137.217.210  00e0-fc01-0203            I -         Ethernet1/0/0
10.137.216.1    0025-9e38-a09e  20        D-0         Ethernet1/0/0
10.137.217.208  00e0-fc01-0205  16        D-0         Ethernet1/0/0
10.2.2.1        00e0-fc99-9999            I -         Eth-Trunk0
10.6.3.34       00e0-fc01-0204            I -         Ethernet2/0/0.1
192.168.20.1    00e0-fc99-9999            I -         Vlanif100
10.0.0.1        00e0-fc99-9999            I -         Vlanif200
--------------------------------------------------------------------------------
Total:7         Dynamic:2       Static:0    Interface:5
```

Table 8-11 Description of the display arp dynamic command output

Item	Description
IP ADDRESS	IP address in the ARP entry.
MAC ADDRESS	MAC address in the ARP entry. If the field is Incomplete, the entry is a fake ARP entry. If a large number of ARP Miss messages are sent to the upper-layer software, the system resources will be exhausted in processing the ARP Miss messages. To resolve this problem, the system automatically generates ARP fake entries instead of ARP entries. You can run the **arp-fake expire-time** command to configure the aging time of fake ARP entries.
EXPIRE(M)	Remaining lifetime of ARP entries, in minutes.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
TYPE	ARP entry type and slot ID of the LPU that obtains the entry. The entry type contains 3 bits. The first bit can be any of the following: • I: Interface, indicating the MAC address of the interface • D: Dynamic, indicating the dynamic entry obtained through the ARP packet • S: Static, indicating the static entry obtained through static configuration The second bit can only be F, indicating that the ARP entry has been reported to the routing module, the route to this IP address has been calculated, and the entry in the FIB has been updated. **NOTE** If the entry is not reported to the routing module, this field displays "-". For the ARP entry with the type as "I", this flag bit does not exist. The third bit indicates the slot ID of the LPU that obtains the entry. **NOTE** For the ARP entry with the type as "I" or "S", this field displays "-".
VPN-INSTANCE	Name of the VPN instance to which the ARP entry belongs. The value is set using the **ip vpn-instance** command.
INTERFACE	Type and number of the interface that has learnt ARP entries.
VLAN/CEVLAN	ID of the VLAN to which the ARP entry belongs. The value is set using the **vlan** command.

Total	Total number of ARP entries in the ARP mapping table.
Dynamic	Number of dynamic ARP entries in the ARP mapping table.
Static	Number of static ARP entries in the ARP mapping table.
Interface	Number of ARP entries in the ARP mapping table on the local interface.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

8.2.14 display arp
8.2.16 display arp interface
8.2.20 display arp network
8.2.22 display arp static
8.2.23 display arp statistics
8.2.31 reset arp

8.2.19 display arp dynamic vlan

Function

The **display arp dynamic vlan** command displays dynamic Address Resolution Protocol (ARP) entries that a device has generated on a specified VLAN.

Format

display arp dynamic [**vlan** *vlan-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays the dynamic ARP entries that a device has generated on a specified VLAN. If this parameter is not specified, all dynamic ARP entries that a device has generated are displayed.	The value is an integer ranging from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To monitor dynamic ARP or locate a fault if dynamic ARP goes faulty on a device, run the **display arp dynamic vlan** command to view dynamic ARP entries. The **display arp dynamic vlan** command displays dynamic ARP entries that a device has generated. You can locate the fault based on the command output.

Example

Display dynamic ARP entries that a device has generated on VLAN 10.

```
<Huawei> display arp dynamic vlan 10
```


Copyright © Huawei Technologies Co., Ltd.

```
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                VLAN/CEVLAN
------------------------------------------------------------------------------
172.16.1.1      0000-c10b-5f77          I -         Vlanif10
172.16.1.2      00e0-4c77-5e3c  20      D-0         GE1/0/1
                                10/-
172.16.1.3      0025-9e36-e8a6  14      D-0         GE1/0/2
                                10/-
172.16.1.4      00e0-fcd5-c860  19      D-0         GE1/0/3
                                10/-
------------------------------------------------------------------------------
Total:4         Dynamic:3       Static:0    Interface:1     Remote:0
```

Table 8-12 Description of the **display arp dynamic vlan** command output

Item	Description
IP ADDRESS	IP address in an ARP entry.
MAC ADDRESS	MAC address in an ARP entry. If the field is Incomplete, the entry is a fake ARP entry. If a large number of ARP Miss messages are sent to the upper-layer software, the system resources will be exhausted in processing the ARP Miss messages. To resolve this problem, the system automatically generates ARP fake entries instead of ARP entries. You can run the **arp-fake expire-time** command to configure the aging time of fake ARP entries.
EXPIRE(M)	Remaining lifetime of an ARP entry, in minutes.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
TYPE	Entry type and number of the slot that obtains the entry. The entry type contains 3 bits. • The first bit can be as follows: – I: Interface, indicating the MAC address of the interface – D: Dynamic, indicating the dynamic entry obtained through the ARP packet – S: Static, indicating the static entry obtained through static configuration – R: Remote, indicating the ARP entry obtained through remote backup • The second bit can only be F, indicating that the entry is reported to the routing module, the route to this IP address is calculated, and the entries in the FIB are correspondingly updated. If the entry is not reported to the routing module, this field displays "-". For the ARP entry with the type as "I", this flag bit does not exist. **NOTE** VLANIF interface and sub-interfaces for VLAN tag termination (including QinQ termination sub-interfaces and Dolt1q termination sub-interfaces) on devices report learned ARP entries to the routing module to generate 32-bit host routes (routes destined for complete host addresses). The host routes are accurate and can be used for packet forwarding. Because the forwarding model of the two types of interfaces requires accurate forwarding paths. However, the outbound interfaces of VLANIF interface routes are VLANIF interfaces. VLANIF interfaces are virtual interfaces that may correspond to multiple physical interfaces, and as a result, such routes cannot be used for packet forwarding. Therefore, the VLANIF interfaces report learned ARP entries to the routing module to generate host routes. As for sub-interfaces for VLAN tag termination, they may correspond to multiple VLANs, and the forwarding model requires that packets be sent to a specified VLAN. Therefore, the sub-interfaces for VLAN tag termination also report learned ARP entries to the routing module to generate host routes. • The third bit indicates the number of the slot that obtains this entry.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	NOTE For the ARP entry with the type as "I" or "S", this field displays "-".
VPN-INSTANCE	Name of the VPN instance to which the ARP entry belongs.
INTERFACE	Type and number of the interface on which the ARP entry is generated.
VLAN	ID of the VLAN to which the ARP entry belongs.
Total	Total number of ARP entries.
Dynamic	Number of dynamic ARP entries.
Static	Number of static ARP entries.
Interface	Number of ARP entries on the interface.
Remote	Number of remote backup ARP entries.

8.2.20 display arp network

Function

The **display arp network** command displays ARP mapping entries of a specified network segment.

Format

display arp network *net-number* [*net-mask*] [**dynamic** | **static**]

Parameters

Parameter	Description	Value
net-number	Specifies the network ID.	The value is in dotted decimal notation.
net-mask	Specifies the subnet mask.	The value is in dotted decimal notation or a decimal number ranging from 1 to 32.
dynamic	Displays dynamic ARP entries of a specified network segment.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
static	Displays static ARP entries of a specified network segment.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display all ARP entries of the network segment with network ID 10.10.0.0 and subnet mask 255.255.0.0.

```
<Huawei> display arp network 10.10.0.0 255.255.0.0
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE       INTERFACE   VPN-INSTANCE
                                VLAN/CEVLAN PVC
--------------------------------------------------------------------------------
10.10.20.9      0018-2000-0083          I -        Vlanif10
10.10.10.6      0018-2000-0083          I -        Vlanif20
--------------------------------------------------------------------------------
Total:2         Dynamic:0       Static:0     Interface:2
```

Table 8-13 Description of the display arp network command output

Item	Description
IP ADDRESS	IP address in the ARP entry.
MAC ADDRESS	MAC address in the ARP entry. If the field is Incomplete, the entry is a fake ARP entry. If a large number of ARP Miss messages are sent to the upper-layer software, the system resources will be exhausted in processing the ARP Miss messages. To resolve this problem, the system automatically generates ARP fake entries instead of ARP entries. You can run the **arp-fake expire-time** command to configure the aging time of fake ARP entries.
EXPIRE(M)	Remaining lifetime of the ARP entry, in minutes.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
TYPE	ARP entry type and slot ID of the LPU that obtains the entry. The entry type contains 3 bits. The first bit can be any of the following: • I: Interface, indicating the MAC address of the interface • D: Dynamic, indicating the dynamic entry obtained through the ARP packet • S: Static, indicating the static entry obtained through static configuration The second bit can only be F, indicating that the ARP entry has been reported to the routing module, the route to this IP address has been calculated, and the entry in the FIB has been updated. **NOTE** If the entry is not reported to the routing module, this field displays "-". For the ARP entry with the type as "I", this flag bit does not exist. The third bit indicates the slot ID of the LPU that obtains the entry. **NOTE** For the ARP entry with the type as "I" or "S", this field displays "-".
VPN-INSTANCE	Name of the VPN instance to which the ARP entry belongs. The value is set using the **ip vpn-instance** command.
INTERFACE	Type and number of the interface that has learnt ARP entries.
VLAN/CEVLAN	ID of the VLAN to which the ARP entry belongs. The value is set using the **vlan** command.
PVC	Interface where the PVC exists and the corresponding VPI/VCI.
Total	Total number of ARP entries in the ARP mapping table.
Dynamic	Number of dynamic ARP entries in the ARP mapping table.
Static	Number of static ARP entries in the ARP mapping table.
Interface	Number of ARP entries in the ARP mapping table on the local interface.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

8.2.12 arp static
8.2.18 display arp dynamic
8.2.16 display arp interface
8.2.22 display arp static
8.2.23 display arp statistics
8.2.31 reset arp

8.2.21 display arp packet statistics

Function

The **display arp packet statistics** command displays the statistics on ARP packets.

Format

display arp packet statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To locate and rectify ARP faults, you can run this command to the statistics on ARP packets.

Example

Display the statistics on ARP packets.

```
<Huawei> display arp packet statistics
ARP Pkt Received:   sum  10088
ARP Learnt Count:   sum     52
ARP Pkt Discard For Limit:   sum      0
ARP Pkt Discard For SpeedLimit:   sum     31
ARP Pkt Discard For Proxy Suppress:   sum    307
ARP Pkt Discard For Other:   sum   9274
```

 Copyright © Huawei Technologies Co., Ltd.

Table 8-14 Description of the display arp packet statistics command output

Item	Description
ARP Pkt Received	Number of the received ARP packets.
ARP Learnt Count	Times of ARP learning.
ARP Pkt Discard For Limit	Number of ARP packets discarded due to the ARP entry limit.
ARP Pkt Discard For SpeedLimit	Number of ARP packets discarded when the number of ARP packets from a specified source IP address exceeds the limit.
ARP Pkt Discard For Proxy Suppress	Number of packets discarded for the speed limit.
ARP Pkt Discard For Other	Number of the packets discarded due to other causes.

8.2.22 display arp static

Function

The **display arp static** command displays all static ARP mapping entries.

Format

display arp static

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display all static ARP entries.

```
<Huawei> display arp static
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE       INTERFACE   VPN-INSTANCE
```

 Copyright © Huawei Technologies Co., Ltd.

```
                                VLAN/CEVLAN PVC
--------------------------------------------------------------------------------
10.1.2.1        0023-0045-0067          S--
--------------------------------------------------------------------------------
Total:1         Dynamic:0       Static:1     Interface:0
```

Table 8-15 Description of the display arp static command output

Item	Description
IP ADDRESS	IP address in the ARP entry.
MAC ADDRESS	MAC address in the ARP entry.
EXPIRE(M)	Remaining lifetime of ARP entries, in minutes.
TYPE	ARP entry type and slot ID of the LPU that obtains the entry. The entry type contains 3 bits. The first bit can be any of the following: • I: Interface, indicating the MAC address of the interface • D: Dynamic, indicating the dynamic entry obtained through the ARP packet • S: Static, indicating the static entry obtained through static configuration The second bit can only be F, indicating that the ARP entry has been reported to the routing module, the route to this IP address has been calculated, and the entry in the FIB has been updated. **NOTE** If the entry is not reported to the routing module, this field displays "-". For the ARP entry with the type as "I", this flag bit does not exist. The third bit indicates the slot ID of the LPU that obtains the entry. **NOTE** For the ARP entry with the type as "I" or "S", this field displays "-".
VPN-INSTANCE	Name of the VPN instance to which the ARP entry belongs. The value is set using the **ip vpn-instance** command.
INTERFACE	Type and number of the interface that has learnt ARP entries.
VLAN/CEVLAN	ID of the VLAN to which the ARP entry belongs. The value is set using the **vlan** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
PVC	Interface where the PVC exists and the corresponding VPI/VCI.

Total	Total number of ARP entries in the ARP mapping table.
Dynamic	Number of dynamic ARP entries in the ARP mapping table.
Static	Number of static ARP entries in the ARP mapping table.
Interface	Number of ARP entries in the ARP mapping table on the local interface.

Related Topics

8.2.12 arp static
8.2.18 display arp dynamic
8.2.16 display arp interface
8.2.20 display arp network
8.2.23 display arp statistics
8.2.31 reset arp

8.2.23 display arp statistics

Function

The **display arp statistics** command displays ARP entry statistics.

Format

display arp statistics { **all** | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
all	Displays ARP entry statistics of the system.	-
interface *interface-type interface-number*	Displays ARP entry statistics of a specified interface.	-

Views

All views

Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

To monitor ARP entries or locate the faults in ARP, you can run this command to check ARP entry statistics.

Example

Display ARP entry statistics.

```
<Huawei> display arp statistics all
Dynamic:1       Static:0
```

Table 8-16 Description of the display arp statistics all command output

Item	Description
Dynamic	Number of dynamic ARP entries.
Static	Number of static ARP entries.

8.2.24 display arp track

Function

The **display arp track** command displays changes of outbound interfaces in ARP entries learned by a VLANIF interface.

Format

display arp track

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If the outbound interfaces change in ARP entries learned by a VLANIF interface, traffic may be interrupted. In this case, run the **display arp track** command to check changes of outbound interfaces and time of changes.

Precautions

After the **display arp track** command is executed, changes of ARP entries are displayed in the following situations:

- Outbound interfaces in dynamic ARP entries learnt by the VLANIF interface change to other interfaces.
- No outbound interface is specified in the static ARP entries. The outbound interface changes to other interfaces.
- Dynamic ARP entries or static ARP entries in which no VLAN ID or outbound interface is specified are deleted.

Changes of ARP entries cannot be displayed in the following situations:

- ARP entries change on a non-VLANIF interface.
- New ARP entries are learnt.
- The VLAN ID and outbound interface are manually specified in static ARP entries.

Example

Display changes of ARP entries.

```
<Huawei> display arp track
Operate Flags: M - Modify, D - Delete
--------------------------------------------------------------------------------
Op IP-Address  MAC-Address     VLAN   Old-Port    New-Port    System-Time
--------------------------------------------------------------------------------
M  10.1.1.1    0001-0001-0001  1000   Ethernet2/0/0  Ethernet1/0/2  2017-08-19 12:10:12
D  10.2.1.100  0003-0003-0003  300              Ethernet1/0/3  2017-08-19 12:12:12
```

Table 8-17 Description of the display arp track command output

Item	Description
Op	Operation identifier. • M: Modify, indicating that the outbound interface changes. • D: Delete, indicating that the ARP entry is deleted.
IP-Address	IP address in the ARP entry.
MAC-Address	MAC address in the ARP entry.
VLAN	ID of the VLAN to which the VLANIF interface belongs.
Old-Port	Original outbound interface in the ARP entry.
New-Port	New outbound interface in the ARP entry.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
System-Time	System time when the outbound interface changes.

8.2.25 display arp vpn-instance

Function

The **display arp vpn-instance** command displays ARP entries of a specified VPN instance.

Format

display arp vpn-instance *vpn-instance-name* [**dynamic** | **static**]

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the VPN instance name.	The value must be an existing VPN instance.
dynamic	Displays dynamic ARP entries.	-
static	Displays static ARP entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To monitor dynamic ARP entries or locate the faults in ARP, you can run this command to check the ARP entries.

Example

Display all the ARP entries of VPN r1.

```
<Huawei> display arp vpn-instance r1
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE       INTERFACE   VPN-INSTANCE
                                          VLAN/CEVLAN PVC
--------------------------------------------------------------------------------
192.168.1.11    0000-0a41-0201          I -        Eth1/0/0       r1
192.168.1.1     0000-0a41-0200  12      D-6        Eth1/0/0       r1
--------------------------------------------------------------------------------
Total:2         Dynamic:1       Static:0    Interface:1
```

 Copyright © Huawei Technologies Co., Ltd.

Table 8-18 Description of the display arp vpn-instance command output

Item	Description
IP ADDRESS	IP address in the ARP entry.
MAC ADDRESS	MAC address in the ARP entry. If the field is Incomplete, the entry is a fake ARP entry. If a large number of ARP Miss messages are sent to the upper-layer software, the system resources will be exhausted in processing the ARP Miss messages. To resolve this problem, the system automatically generates ARP fake entries instead of ARP entries. You can run the **arp-fake expire-time** command to configure the aging time of fake ARP entries.
EXPIRE(M)	Remaining lifetime of the ARP entry, in minutes.
TYPE	ARP entry type and slot ID of the LPU that obtains the entry. The entry type contains 3 bits. The first bit can be any of the following: • I: Interface, indicating the MAC address of the interface • D: Dynamic, indicating the dynamic entry obtained through the ARP packet • S: Static, indicating the static entry obtained through static configuration The second bit can only be F, indicating that the entry is reported to the routing module, the route to this IP address is calculated, and entries in the FIB are correspondingly updated. **NOTE** If the entry is not reported to the routing module, this field displays "-". For the ARP entry with the type as "I", this flag bit does not exist. The third bit indicates the slot ID of the LPU that obtains the entry. **NOTE** For the ARP entry with the type as "I" or "S", this field displays "-".
VPN-INSTANCE	Name of the VPN instance to which the ARP entry belongs. The value is set using the **ip vpn-instance** command.
INTERFACE	Type and number of the interface that has learnt ARP entries.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
VLAN/CEVLAN	ID of the VLAN to which the ARP entry belongs. The value is set using the **vlan** command.
PVC	Interface where the PVC exists and the corresponding VPI/VCI.
Total	Number of ARP entries.
Dynamic	Number of dynamic ARP entries.
Static	Number of static ARP entries.
Interface	Number of ARP entries of the local interface.

Related Topics

8.2.12 arp static

8.2.16 display arp interface

8.2.31 reset arp

8.2.26 display mac-address multiport

Function

The **display mac-address multiport** command displays the configured multi-interface MAC address entries.

Format

display mac-address multiport [[*mac-address*] **vlan** *vlan-id*] [**total-number**]

Parameters

Parameter	Description	Value
mac-address	Displays the specified multi-interface MAC address entry.	The value is in H-H-H format. An H contains 1 to 4 hexadecimal digits.
vlan *vlan-id*	Displays multi-interface MAC address entries in the specified VLAN.	The value is an integer that ranges from 1 to 4094.
total-number	Displays the total number of multi-interface MAC address entries.	-

Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the configured multi-interface MAC address entries. If no MAC address or VLAN is specified, the system displays all multi-interface MAC address entries. You can configure multi-interface MAC address entries using the **8.2.30 mac-address multiport interface** or **8.2.29 mac-address multiport** command.

Example

Display multi-interface MAC address entries in VLAN 100.

```
<Huawei> display mac-address multiport vlan 100
--------------------------------------------------------------------------------
MAC Address       VLANID    Out-Interface
--------------------------------------------------------------------------------
03bf-2100-2200    100       Ethernet5/0/1
                            Ethernet5/0/2
                                  2 port(s)
--------------------------------------------------------------------------------
 Total Group(s) : 1
```

Display the multi-interface MAC address entry matching MAC address 03bf-0a80-f6fc in VLAN 100.

```
<Huawei> display mac-address multiport 03bf-0a80-f6fc vlan 100
--------------------------------------------------------------------------------
MAC Address       VLANID    Out-Interface
--------------------------------------------------------------------------------
03bf-2100-2200    100       Ethernet5/0/1
                            Ethernet5/0/2
                                  2 port(s)
--------------------------------------------------------------------------------
 Total Group(s) : 1
```

Display the number of configured multi-interface MAC address entries.

```
<Huawei> display mac-address multiport total-number
Total number of mac-address : 1
```

Table 8-19 Description of the display mac-address multiport command output

Item	Description
MAC Address	Destination MAC address.
VLANID	VLAN to which the outbound interface belongs.
Out-Interface	Outbound interface.
Total Group(s)	Total number of multi-interface MAC address entries.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Total number of mac-address	Total number of multi-interface MAC address entries.

Related Topics

8.2.29 mac-address multiport
8.2.30 mac-address multiport interface

8.2.27 display snmp-agent trap feature-name arp all

Function

The **display snmp-agent trap feature-name arp all** command displays all trap messages of the ARP module.

Format

display snmp-agent trap feature-name arp all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The Simple Network Management Protocol (SNMP) is a standard network management protocol widely used on TCP/IP networks. It uses a central computer (a network management station) that runs network management software to manage network elements. The management agent on the network element automatically reports traps to the network management station. After that, the network administrator immediately takes measures to resolve the problem.

After running the **snmp-agent trap enable feature-name arp** command to enable or disable a trap function of the ARP module, run the **display snmp-agent trap feature-name arp all** command to check the status of all trap functions of the ARP module.

Example

Display all trap messages of the ARP module.

```
<Huawei>display snmp-agent trap feature-name arp all
------------------------------------------------------------------------------
```


Copyright © Huawei Technologies Co., Ltd.

```
Feature name: ARP
Trap number : 6
--------------------------------------------------------------------------------
Trap name                       Default switch status   Current switch status
hwEthernetARPSpeedLimitAlarm    on                      on
hwEthernetARPThresholdExceedAlarm
                                on                      on
hwEthernetARPThresholdResumeAlarm
                                on                      on
hwEthernetARPIPConflictEvent    on                      on
hwEthernetARPLearnStopAlarm     on                      on
hwEthernetARPLearnResumeAlarm   on                      on
```

Table 8-20 Description of the **display snmp-agent trap feature-name arp all** command output

Item	Description
Feature name	Name of the module to which a trap message belongs.
Trap number	Number of trap messages.
Trap name	Name of a trap message of the ARP module: • hwEthernetARPSpeedLimitAlarm: alarm of ARP speed limit. It is a non-excessive trap. • hwEthernetARPThresholdExceedAlarm: alarm of the number of ARP entries exceeding the upper threshold. • hwEthernetARPThresholdResumeAlarm: alarm of the number of ARP entries falling below the upper threshold. • hwEthernetARPIPConflictEvent: alarm of the IP address conflict. • hwEthernetARPLearnStopAlarm: alarm of stopping learning ARP entries because the board memory usage reaches the threshold. • hwEthernetARPLearnResumeAlarm: clear alarm of stopping learning ARPpackets because the board memory usage falls below the threshold.
Default switch status	Status of the default trap switch: • on: indicates that the trap function is enabled. • off: indicates that the trap function is disabled.
Current switch status	Status of the current trap switch: • on: indicates that the trap function is enabled. • off: indicates that the trap function is disabled.

Related Topics

8.2.33 snmp-agent trap enable feature-name arp

 Copyright © Huawei Technologies Co., Ltd.

8.2.28 l2-topology detect enable

Function

The **l2-topology detect enable** command enables Layer 2 topology detection.

The **undo l2-topology detect enable** command disables Layer 2 topology detection.

By default, Layer 2 topology detection is disabled.

Format

l2-topology detect enable

undo l2-topology detect enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the **l2-topology detect enable** command is run, all ARP entries in the VLAN are updated if the Layer 2 interface changes from Down to Up.

Example

Enable Layer 2 topology detection.

```
<Huawei> system-view
[Huawei] l2-topology detect enable
```

8.2.29 mac-address multiport

Function

The **mac-address multiport** command configures a multi-interface MAC address entry in the interface view.

The **undo mac-address multiport** command deletes a multi-interface MAC address entry in the interface view.

By default, no multi-interface MAC address entry is configured.

 Copyright © Huawei Technologies Co., Ltd.

Format

mac-address multiport *mac-address* **vlan** *vlan-id*

undo mac-address multiport *mac-address* **vlan** *vlan-id*

Parameters

Parameter	Description	Value
mac-address	Specifies a MAC address.	The value is in H-H-H format. An H contains 1 to 4 hexadecimal digits.
vlan *vlan-id*	Specifies a VLAN to which an interface belongs.	The value is an integer that ranges from 1 to 4094.

Views

Ethernet interface view, GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All servers in an NLB group share a virtual IP address and a virtual MAC address. When a device functions as the access gateway and directly connects to the NLB group, the device needs to forward packets destined for the virtual IP address to all servers in the NLB group. You can run the **mac-address multiport** or **8.2.30 mac-address multiport interface** command to configure a multi-interface MAC address entry, and run the **8.2.12 arp static** command to configure a short static ARP entry. After the configurations, the device determines the virtual MAC address matching the virtual IP address and the VLAN to which the NLB servers belong. Then the device determines the outbound interfaces by searching the MAC address table based on the virtual MAC address and VLAN. The device can communicate with the NLB servers.

Prerequisites

A VLAN has been created, and the interface has been added to the VLAN.

Precautions

The VLAN cannot be a super-VLAN, sub-VLAN, MUX VLAN, or control VLAN of a SEP segment.

When you run the **mac-address multiport** command to configure a multi-interface MAC address entry, ensure that the specified MAC address and VLAN ID are simultaneously different from those in a static MAC address entry or a blackhole MAC address entry.

Copyright © Huawei Technologies Co., Ltd.

Example

Configure a multi-interface MAC address entry with the destination MAC address being 03bf-2100-2200 on Ethernet2/0/0 in VLAN 100.

```
<Huawei> system-view
[Huawei] vlan batch 100
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port link-type access
[Huawei-Ethernet2/0/0] port default vlan 100
[Huawei-Ethernet2/0/0] mac-address multiport 03bf-2100-2200 vlan 100
```

Related Topics

8.2.30 mac-address multiport interface

8.2.26 display mac-address multiport

8.2.30 mac-address multiport interface

Function

The **mac-address multiport interface** command configures a multi-interface MAC address entry in the system view.

The **undo mac-address multiport interface** command deletes a multi-interface MAC address entry in the system view.

By default, no multi-interface MAC address entry is configured on a device.

Format

mac-address multiport *mac-address* **interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-5> **vlan** *vlan-id*

undo mac-address multiport *mac-address* **interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-5> **vlan** *vlan-id*

undo mac-address multiport { **all** | [*mac-address*] **vlan** *vlan-id* }

Parameters

Parameter	Description	Value
mac-address	Specifies a MAC address.	The value is in H-H-H format. An H contains 1 to 4 hexadecimal digits.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface-type interface-number1 [**to** *interface-type interface-number2*]	Specifies the interface type and number. • *interface-type* specifies the interface type. • *interface-number1* specifies the number of the first interface for which a multi-interface MAC address entry needs to be configured. • *interface-number2* specifies the number of the last interface for which a multi-interface MAC address entry needs to be configured. The value of *interface-number2* must be greater than that of *interface-number1*, and the two values determine an interface range. On AR1200, AR2200 AR3600, and AR3200, the specified interfaces must be located on the same card.	-
vlan *vlan-id*	Specifies a VLAN to which interfaces belong.	The value is an integer that ranges from 1 to 4094.
all	Specifies all multi-interface MAC address entries.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All servers in an NLB group share a virtual IP address and a virtual MAC address. When a device functions as the access gateway and directly connects to the NLB group, the device needs to forward packets destined for the virtual IP address to all servers in the NLB group. You can run the **mac-address multiport interface** or **8.2.29 mac-address multiport** command to configure a multi-interface MAC address entry, and run the **8.2.12 arp static** command to configure a short static ARP entry. After the configurations, the device determines the virtual MAC address matching the virtual IP address and the VLAN to which the NLB servers belong. Then the device determines the outbound interfaces by searching the MAC address table based on the virtual MAC address and VLAN. The device can communicate with the NLB servers.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

A VLAN has been created, and the interfaces have been added to the VLAN.

Precautions

The VLAN cannot be a super-VLAN, sub-VLAN, MUX VLAN, or control VLAN of a SEP segment.

When you run the **mac-address multiport interface** command to configure a multi-interface MAC address entry, ensure that the specified MAC address and VLAN ID are simultaneously different from those in a static MAC address entry or a blackhole MAC address entry.

Example

Configure a multi-interface MAC address entry with the destination MAC address being 03bf-2100-2200 and outbound interfaces being Ethernet2/0/0 and Ethernet2/0/1 in VLAN 100.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port link-type access
[Huawei-Ethernet2/0/0] quit
[Huawei] interface ethernet 2/0/1
[Huawei-Ethernet2/0/1] port link-type access
[Huawei-Ethernet2/0/1] quit
[Huawei] vlan 100
[Huawei-vlan100] port ethernet 2/0/0 to 2/0/1
[Huawei-vlan100] quit
[Huawei] mac-address multiport 03bf-2100-2200 interface ethernet 2/0/0 to ethernet 2/0/1 vlan 100
```

Related Topics

8.2.29 mac-address multiport

8.2.26 display mac-address multiport

8.2.31 reset arp

Function

The **reset arp** command deletes ARP entries in the ARP mapping table.

Format

reset arp { **dynamic** [**ip** *ip-address* [**vpn-instance** *vpn-instance-name*]] | **interface** *interface-type interface-number* [**ip** *ip-address*] | **static** }

Parameters

Parameter	Description	Value
dynamic	Deletes dynamic ARP entries.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. • *interface-type* specifies the type of the interface. • *interface-number* specifies the number of the interface.	-
ip *ip-address*	Deletes dynamic ARP entries of a specified interface and with a specified IP address. If an interface learns excessive ARP entries, you can specify this parameter to delete a specified ARP entry.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specify the vpn-instance name.	The value must be an existing VPN instance.
static	Deletes static ARP entries.Static ARP entries cannot be restored after being cleared. Exercise caution when you clear static ARP entries.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a device is attacked, it learns a large number of invalid ARP entries. In this case, you can use this command to delete ARP entries.

Precautions

- The **reset arp** command deletes mappings between IP addresses and MAC addresses. As a result, users may fail to access some nodes.

Example

Delete dynamic ARP entries in the ARP mapping table.

```
<Huawei> reset arp dynamic
```

Delete ARP entries of Ethernet2/0/0 with the IP address 10.1.1.1 in the ARP mapping table.

```
<Huawei> reset arp interface ethernet 2/0/0 ip 10.1.1.1
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

8.2.16 display arp interface

8.2.32 reset arp packet statistics

Function

The **reset arp packet statistics** command clears the statistics on ARP packets.

Format

reset arp packet statistics

Parameters

None

Views

User view

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display arp packet statistics** command to display the statistics on ARP packets. To obtain correct statistics, run the **reset arp packet statistics** command to clear existing statistics first.

The **reset arp packet statistics** command clears the ARP packet statistics only on the main control board.

Example

Clear the statistics on all ARP packets.

```
<Huawei> reset arp packet statistics
```

8.2.33 snmp-agent trap enable feature-name arp

Function

The **snmp-agent trap enable feature-name arp** command enables the trap function for the ARP module.

The **undo snmp-agent trap enable feature-name arp** command disables the trap function for the ARP module.

By default, the trap function is enabled for the ARP module.

 Copyright © Huawei Technologies Co., Ltd.

Format

snmp-agent trap enable feature-name arp [**trap-name** { **hwethernetarpspeedlimitalarm** | **hwethernetarpthresholdexceedalarm** | **hwethernetarpthresholdresumealarm** | **hwethernetarpipconflictevent** }]

undo snmp-agent trap enable feature-name arp [**trap-name** { **hwethernetarpspeedlimitalarm** | **hwethernetarpthresholdexceedalarm** | **hwethernetarpthresholdresumealarm** | **hwethernetarpipconflictevent** }]

Parameters

Parameter	Description	Value
trap-name	Enables the traps of ARP events of specified types.	-
hwethernetarpspeedlimitalarm	Enables the alarm of ARP speed limit. It is a non-excessive trap.	-
hwethernetarpthresholdexceedalarm	Enables the alarm of the number of ARP entries exceeding the upper threshold.	-
hwethernetarpthresholdresumealarm	Enables the alarm of the number of ARP entries falling below the upper threshold.	-
hwethernetarpipconflictevent	Enables the alarm of IP address conflict.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

If you do not specify **trap-name**, all traps of the ARP module will be enabled.

Example

Enables the trap function of ARP speed limit.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name arp trap-name hwethernetarpspeedlimitalarm
```

8.3 DHCP Configuration Commands

NOTE

Wireless interfaces cannot function as DHCP clients or BOOTP clients.

 Copyright © Huawei Technologies Co., Ltd.

8.3.1 alarm ip-used percentage

Function

The **alarm ip-used percentage** command configures the percentage of the alarms indicating that the addresses in an address pool are used up, and the percentage of the clear alarms.

The **undo alarm ip-used percentage** command restores the default percentages of the alarms and clear alarms.

By default, the percentage of the alarms indicating that the addresses in an IP address pool are used up is 100%, and the percentage of the clear alarms is 50%.

Format

alarm ip-used percentage *alarm-resume-percentage alarm-percentage*

undo alarm ip-used percentage

Parameters

Parameter	Description	Value
alarm-resume-percentage	Specifies the percentage of the clear alarms.	The value is an integer that ranges from 1 to 100. The default value is **50**. **NOTE** The percentage of the clear alarms cannot exceed that of the alarms.
alarm-percentage	Specifies the percentage of the alarms indicating that the addresses in an address pool are used up.	The value is an integer that ranges from 1 to 100. The default value is **100**.

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the addresses in an IP address pool are used up, alarms are sent to notify the administrator.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

The percentage of the clear alarms cannot exceed that of the alarms.

Example

Configure the percentage of the alarms indicating that the addresses in an address pool are used up, and the percentage of the clear alarms in the IP address pool view.

```
<Huawei> system-view
[Huawei] ip pool p1
[Huawei-ip-pool-p1] alarm ip-used percentage 80 90
```

8.3.2 bootfile

Function

The **bootfile** command configures the name of the startup configuration file for a DHCP client.

The **undo bootfile** command deletes the configured name of the startup configuration file for a DHCP client.

By default, the startup configuration file name is not configured for a DHCP client.

Format

bootfile *bootfile*

undo bootfile

Parameters

Parameter	Description	Value
bootfile	Specifies the name of the startup configuration file for a DHCP client.	The value is a string of 1 to 127 case-sensitive characters without spaces.

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on a DHCP server. Besides assigning IP addresses, a DHCP server can also provide the required network configuration parameters, such as

 Copyright © Huawei Technologies Co., Ltd.

the startup configuration file name for the DHCP clients. After the startup configuration file name is configured using the **bootfile** command, the Offer and ACK packets sent from the DHCP server carry this file name. The DHCP client can acquire the startup configuration file from the specified server based on the file name.

Precautions

Usually, the startup configuration file is saved on a specified file server. Therefore, the route between the DHCP client and the file server must be reachable and the ip address or name of the file server must be specified.

Example

In the IP address pool view, configure the name of the startup configuration file as **start.ini** for the DHCP client.

```
<Huawei> system-view
[Huawei] ip pool p1
[Huawei-ip-pool-p1] bootfile start.ini
```

In the DHCP Option template view, configure the name of the startup configuration file as **start.ini** for the DHCP client.

```
<Huawei> system-view
[Huawei] dhcp option template template1
[Huawei-dhcp-option-template-template1] bootfile start.ini
```

Related Topics

8.3.83 ip pool (system view)

8.3.20 dhcp option template

8.3.3 conflict auto-recycle interval

Function

The **conflict auto-recycle interval** command enables automatic reclaim of conflicting IP addresses in the global address pool and configures the interval for the automatic reclaim.

The **undo conflict auto-recycle interval** command disables automatic reclaim of conflicting IP addresses in the global address pool and deletes the configured interval for the automatic reclaim.

By default, automatic reclaim of conflicting IP addresses in the global address pool is disabled.

Format

conflict auto-recycle interval day *day* [**hour** *hour* [**minute** *minute*]]

undo conflict auto-recycle interval

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
day *day*	Specifies the interval for the automatic reclaim, in days.	The value is an integer that ranges from 0 to 999, in days. The default value is 0.
hour *hour*	Specifies the interval for the automatic reclaim, in hours.	The value is an integer that ranges from 0 to 23, in hours. The default value is 0.
minute *minute*	Specifies the interval for the automatic reclaim, in minutes.	The value is an integer that ranges from 0 to 59, in minutes. The default value is 0.

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on a DHCP server. When a DHCP server allocates IP addresses to clients, IP address conflict may occur because IP addresses of some hosts have been manually configured. In this case, the DHCP server considers these IP addresses as conflicting IP addresses, and allocates available IP addresses from the conflicting IP addresses to clients only after available IP addresses in the address pool are used up. To reclaim conflicting IP addresses promptly, the administrator can run the **conflict auto-recycle interval** command to enable automatic reclaim and specify the reclaim interval.

Prerequisites

The global address pool has been created using the **8.3.83 ip pool (system view)** command.

Example

Enable automatic reclaim for conflicting IP addresses in the global address pool **global1**, and set the interval for automatic reclaim to one day.

```
<Huawei> system-view
[Huawei] ip pool global1
[Huawei-ip-pool-global1] conflict auto-recycle interval day 1
```

 Copyright © Huawei Technologies Co., Ltd.

8.3.4 dhcp alarm dhcp-rate enable

Function

Using the **dhcp alarm dhcp-rate enable** command, you can enable the DHCP message checking alarm.

Using the **undo dhcp alarm dhcp-rate enable** command, you can disable the DHCP message checking alarm.

By default, the DHCP message checking alarm is disabled.

Format

dhcp alarm dhcp-rate enable

undo dhcp alarm dhcp-rate enable

Parameters

None

Views

System view, interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After DHCP message checking is enabled, configure the DHCP message checking alarm on an interface. An alarm is generated if the number of discarded DHCP messages on the interface reaches the alarm threshold.

The interfaces supporting this command include Layer 2 GE interfaces, Layer 2 Ethernet interfaces, Layer 2 Eth-Trunk interfaces, Layer 2 port group, Layer 3 GE interfaces, and Layer 3 Ethernet interfaces.

Prerequisites

The following configurations have been performed in sequence:

1. DHCP has been enabled globally by using the **dhcp enable** command.
2. DHCP message checking has been enabled by using the **dhcp check dhcp-rate enable** command.

Follow-up Procedure

Run the **dhcp alarm dhcp-rate threshold** command to set the alarm threshold.

Copyright © Huawei Technologies Co., Ltd.

Example

Enable the DHCP message checking alarm on Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp check dhcp-rate enable
[Huawei-Ethernet2/0/0] dhcp alarm dhcp-rate enable
```

Related Topics

8.3.5 dhcp alarm dhcp-rate threshold

8.3.5 dhcp alarm dhcp-rate threshold

Function

The **dhcp alarm dhcp-rate threshold** command sets the alarm threshold for DHCP message checking on an interface.

The **undo dhcp alarm dhcp-rate threshold** command restores the default alarm threshold.

The **dhcp alarm dhcp-rate enable threshold** command enables a device to generate an alarm when the number of discarded DHCP messages reaches the threshold and sets the corresponding alarm threshold.

The **undo dhcp alarm dhcp-rate enable threshold** command disables a device from generating an alarm when the number of discarded DHCP messages reaches the threshold.

By default, a device is not enabled to generate an alarm when the number of discarded DHCP messages reaches the threshold, and the alarm threshold is 100 packets.

Format

dhcp alarm dhcp-rate threshold *threshold*

undo dhcp alarm dhcp-rate threshold

dhcp alarm dhcp-rate enable threshold *threshold*

undo dhcp alarm dhcp-rate enable threshold

Parameters

Parameter	Description	Value
threshold	Specifies the alarm threshold for DHCP message checking on an interface.	The value is an integer ranging from 1 to 1000.

Copyright © Huawei Technologies Co., Ltd.

Views

System view, interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the DHCP message checking alarm is enabled on an interface, set the alarm threshold for DHCP message checking on an interface. An alarm is generated when the number of discarded DHCP messages reaches the alarm threshold on an interface.

Prerequisites

Before running the **dhcp alarm dhcp-rate threshold** command, you must run the **dhcp alarm dhcp-rate enable** command to enable the DHCP message checking alarm.

Precautions

If you set the alarm threshold for DHCP message checking in both the system view and interface view, the alarm threshold configured in the interface view takes effect.

The interfaces supporting this command include Layer 2 GE interfaces, Layer 2 Ethernet interfaces, Layer 2 Eth-Trunk interfaces, Layer 2 port group, Layer 3 GE interfaces, and Layer 3 Ethernet interfaces.

Example

Set the alarm threshold for DHCP message checking to 150 on interface Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp alarm dhcp-rate threshold 150
```

Related Topics

8.3.4 dhcp alarm dhcp-rate enable

8.3.6 dhcp check dhcp-rate enable

Function

The **dhcp check dhcp-rate enable** command enables DHCP packet rate checking.

The **undo dhcp check dhcp-rate enable** command disables DHCP packet rate checking.

By default, DHCP packet rate checking is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Format

In the system view:

dhcp check dhcp-rate enable [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

undo dhcp check dhcp-rate enable [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

In the interface view or VLAN view:

dhcp check dhcp-rate enable

undo dhcp check dhcp-rate enable

Parameters

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] }	Enables DHCP packet rate checking in specified VLANs. • *vlan-id1* specifies the ID of the first VLAN. • *vlan-id2* specifies the ID of the last VLAN. *vlan-id2* and *vlan-id1* determine a VLAN ID range.	• *vlan-id1* is an integer that ranges from 1 to 4094. • *vlan-id2* is an integer that ranges from 1 to 4094. *vlan-id2* must be larger than *vlan-id1*.

Views

System view, VLAN view, Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If attackers send DHCP packets continuously, the protocol stack of the router is affected.

To prevent attackers from sending a large number of DHCP packets, enable DHCP message checking on the router. The router checks the rate of sending DHCP packets including DHCP request and DHCP response packets. Only a certain number of DHCP packets can be sent to the DHCP protocol stack in a certain period of time and excess messages are discarded.

The interfaces supporting this command include Layer 2 GE interfaces, Layer 2 Ethernet interfaces, Layer 2 Eth-Trunk interfaces, Layer 2 port group, Layer 3 GE interfaces, and Layer 3 Ethernet interfaces.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

DHCP has been enabled globally by using the **dhcp enable** command.

Follow-up Procedure

Run the **dhcp check dhcp-rate** command to set the rate of sending DHCP packets.

Example

Enable DHCP packet rate checking in the system view.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp check dhcp-rate enable
```

Enable DHCP packet rate checking in VLAN 100.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] vlan 100
[Huawei-vlan100] dhcp check dhcp-rate enable
```

Related Topics

8.3.18 dhcp enable

8.3.7 dhcp check dhcp-rate

8.3.7 dhcp check dhcp-rate

Function

The **dhcp check dhcp-rate** command sets the checking rate of DHCP messages sent to the DHCP protocol stack.

The **undo dhcp check dhcp-rate** command restores the default checking rate of DHCP messages sent to the DHCP protocol stack.

By default, the checking rate of DHCP messages sent to the DHCP protocol stack is 100 pps.

Format

In the system view:

dhcp check dhcp-rate *rate* [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

undo dhcp check dhcp-rate

In the interface view or VLAN view:

dhcp check dhcp-rate *rate*

undo dhcp check dhcp-rate

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
rate	Specifies the checking rate of DHCP messages sent to the DHCP protocol stack.	The value ranges from 1 to 100, in pps.
vlan { *vlan-id1* [**to** *vlan-id2*] }	Specifies the checking rate of DHCP messages sent from the specified VLAN to the DHCP protocol stack. • *vlan-id1*: specifies the ID of the first VLAN. • *vlan-id2*: specifies the ID of the last VLAN. *vlan-id2* and *vlan-id1* determine a VLAN ID range.	• *vlan-id1* is an integer that ranges from 1 to 4094. • *vlan-id2* is an integer that ranges from 1 to 4094. *vlan-id2* must be larger than *vlan-id1*.

Views

System view, VLAN view, interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After DHCP message checking is enabled, set the checking rate of DHCP messages sent to the DHCP protocol stack. In a period of time, only a certain number of DHCP messages can be sent to the DHCP protocol stack. The DHCP messages that exceed the rate are discarded.

Prerequisites

DHCP message checking has been enabled by using the **dhcp check dhcp-rate enable** command.

Precautions

You can set the checking rate of DHCP messages sent to the DHCP protocol stack in the system view, interface view, or VLAN view. The checking rates configured in the interface view, VLAN view, and system view take effect in descending order of priority.

If you run the **dhcp check dhcp-rate** *rate* command only in the system view, the checking rate of DHCP messages sent to the DHCP protocol stack in the VLAN view and interface view is the same as that configured in the system view.

 Copyright © Huawei Technologies Co., Ltd.

The interfaces supporting this command include Layer 2 GE interfaces, Layer 2 Ethernet interfaces, Layer 2 Eth-Trunk interfaces, Layer 2 port group, Layer 3 GE interfaces, and Layer 3 Ethernet interfaces.

Example

Set the checking rate of DHCP messages to 50 pps.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp check dhcp-rate 50
```

Related Topics

8.3.6 dhcp check dhcp-rate enable

8.3.8 dhcp client class-id (interface view)

Function

The **dhcp client class-id** command sets the Option60 field in the DHCP request packet sent by the DHCP client.

The **undo dhcp client class-id** command deletes the configured Option60 field in the DHCP request packet sent by the DHCP client.

By default, no Option60 field is configured.

Format

dhcp client class-id *class-id*

undo dhcp client class-id

Parameters

Parameter	Description	Value
class-id	Indicates the value of the Option60 field.	The value is a string of 1 to 64 case-sensitive characters.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The DHCP server identifies the devices according to the Option60 field in the DHCP request packet. You can run the **dhcp client class-id** *class-id* command to

 Copyright © Huawei Technologies Co., Ltd.

customize the Option60 field in the DHCP request packet sent from the DHCP client.

After you run the **dhcp client class-id** *class-id* command in the VLANIF interface view, the device that functions as the DHCP client fills the set Option60 in the DHCP request packet on the VLANIF interface.

Example

Set the class-id of a DHCP client to **huawei** on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcp client class-id huawei
```

8.3.9 dhcp client class-id (system view)

Function

The **dhcp client class-id** command is used to set the Option60 field in the DHCP request packet sent by the DHCP client.

The **undo dhcp client class-id** command is used to restore the default value of the Option60 field.

By default, the default value of the Option60 field depends on the device type, which is " huawei *Device Model*".

Format

dhcp client class-id *class-id*

undo dhcp client class-id

Parameters

Parameter	Description	Value
class-id	Indicates the value of the Option60 field.	The value is a string of 1 to 64 case-sensitive characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The DHCP server identifies the devices according to the Option60 field in the DHCP request packet. You can run the **dhcp client class-id** *class-id* command to

 Copyright © Huawei Technologies Co., Ltd.

customize the Option60 field in the DHCP request packet sent from the DHCP client.

Configuration information of the Option60 field is saved in the *storage device*:/dhcp/dhcp-client.options file. By default, the storage device needs to provide more than 80-byte storage space. You can run the **more dhcp/dhcp-client.options** command in the user view to check configuration information of the Option60 field.

After you run the **dhcp client class-id** *class-id* command in the system view, the device that functions as the DHCP client fills the set Option60 in the DHCP request packet sent from all of the interfaces.

Example

Set the class-ID of a DHCP client to **huawei**.

```
<Huawei> system-view
[Huawei] dhcp client class-id huawei
```

8.3.10 dhcp client client-id

Function

The **dhcp client client-id** command configures an identifier for a DHCP client.

The **undo dhcp client client-id** command restores the default identifier of a DHCP client.

By default, the identifier of a DHCP client is the client's MAC address.

Format

dhcp client client-id *client-id*

undo dhcp client client-id

Parameters

Parameter	Description	Value
client-id	Specifies the identifier of a DHCP client.	The value is a string of 2 to 64 case-sensitive characters without spaces.

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The **dhcp client client-id** command configures an identifier for a DHCP client. The identifier is encapsulated into a DHCP Request message. When a DHCP client requests an IP address from a DHCP server, the DHCP server obtains the identifier of the DHCP client and assigns an IP address to the DHCP client with the specified identifier.

Example

Set the identifier of the DHCP client to **huawei_client** on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcp client client-id huawei_client
```

8.3.11 dhcp client expected-lease

Function

The **dhcp client expected-lease** command enables expected lease on a DHCP client.

The **undo dhcp client expected-lease** command disables expected lease on a DHCP client.

By default, expected lease is disabled on the DHCP client.

Format

dhcp client expected-lease *time*

undo dhcp client expected-lease

Parameters

Parameter	Description	Value
time	Specifies an expected lease for a DHCP client.	The value is an integer that ranges from 60 to 864000, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The **dhcp client expected-lease** command applies to DHCP clients. An expected lease can be contained in Option 51 of a DHCP Request message sent to the

 Copyright © Huawei Technologies Co., Ltd.

server. The server compares the expected lease with the lease in the address pool and assigns a shorter lease to the client.

NOTE

When the device functions as the DHCP client, the lease cannot be shorter than 8 seconds. Otherwise, some packets are discarded. Therefore, the lease configured on the peer end DHCP server cannot be shorter than 8 seconds.

Example

Set the expected lease to 7200s on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcp client expected-lease 7200
```

8.3.12 dhcp client gateway-detect

Function

The **dhcp client gateway-detect** command enables gateway detection on a DHCP client.

The **undo dhcp client gateway-detect** command disables gateway detection on a DHCP client.

By default, gateway detection is disabled on a DHCP client.

Format

dhcp client gateway-detect period *period* **retransmit** *retransmit* **timeout** *time*

undo dhcp client gateway-detect

Parameters

Parameter	Description	Value
period *period*	Specifies an interval for gateway detection on a DHCP client.	The value is an integer that ranges from 1 to 86400, in seconds.
retransmit *retransmit*	Specifies the retransmission count of gateway detection on a DHCP client.	The value is an integer that ranges from 1 to 10.
timeout *time*	Specifies the timeout period of gateway detection on a DHCP client.	It is an integer that ranges from 300 to 2000, in milliseconds.

Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp client gateway-detect** command applies to DHCP clients. After a DHCP client obtains an IP address, the **dhcp client gateway-detect** command enables the DHCP client to detect the status of the gateway being used. If the gateway has an incorrect address or the gateway device fails, the DHCP client requests a new IP address from the DHCP server.

Precautions

Gateway detection applies to dual-homed scenarios.

Example

Enable gateway detection on GE1/0/0 of the DHCP client. Set the detection interval to 3600s, retransmission count to 3, and timeout period to 500 ms.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcp client gateway-detect period 3600 retransmit 3 timeout 500
```

8.3.13 dhcp client default-route preference

Function

The **dhcp client default-route preference** command configures the default route preference that a DHCP server delivers to a DHCP client.

The **undo dhcp client default-route preference** command restores the default value of the default route preference that a DHCP server delivers to a DHCP client.

By default, the default route preference that a DHCP server delivers to a DHCP client is 60.

Format

dhcp client default-route preference *preference-value*

undo dhcp client default-route preference

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
preference-value	Specifies the default route preference.	The value is an integer that ranges from 1 to 255. A smaller value indicates a higher preference.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

A DHCP client can obtain the default route through the DHCP server to dynamically update the routing table. The next-hop address of the default route is the DHCP client's gateway address carried in Option3.

The default route that a DHCP server delivers is the user network router (UNR) route with the default preference 60. You can run the **dhcp client default-route preference** command to change the default route preference.

Example

In the view of VLANIF100, set the default route preference that a DHCP server delivers to a DHCP client to 30.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcp client default-route preference 30
```

8.3.14 dhcp client hostname

Function

The **dhcp client hostname** command configures a host name for a DHCP/BOOTP client.

The **undo dhcp client hostname** command deletes the configured host name of a DHCP/BOOTP client.

By default, no host name is configured for a DHCP/BOOTP client.

Format

dhcp client hostname *hostname*

undo dhcp client hostname

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
hostname	Specifies the name of a DHCP/BOOTP client.	The value is a string of 1 to 64 case-sensitive characters.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A DHCP server must obtain the host name of a client before assigning an IP address to the client. To configure a host name for a DHCP/BOOTP client, run the **dhcp client hostname** command. The host name is used to match the local domain name of the DHCP/BOOTP client.

Follow-up Procedure

After DHCP/BOOTP client is enabled, the device can use DHCP to obtain an IP address.

Example

Set the host name of a DHCP/BOOTP client to **huawei gateway** on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcp client hostname huawei gateway
```

8.3.15 dhcp client renew

Function

The **dhcp client renew** command renews the lease of the IP address obtained by a DHCP client.

Format

dhcp client renew

Parameters

None

Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

This command applies to the following scenarios:

- Manually renewing the lease

  If a DHCP server assigns the original IP address to the client, only the lease is renewed. If another DHCP server assigns an IP address to the client, the client obtains a new IP address and related network parameters.
- Updating the IP address

  When the DHCP client is migrated from a network segment to another network segment and the original IP address lease does not expire, the client needs to update the IP address.

After the **dhcp client renew** command is run, the DHCP client sends a lease renewal request to the DHCP server.

- If the DHCP client receives a positive reply from the server, the client updates the parameters such as the lease duration.
- If the DHCP client receives a negative reply from the server, the client releases the applied parameters and re-applies to the DHCP server for an IP address and other network parameters.
- If no reply is received, the client does not perform any operation.

The **dhcp client renew** command can be normally run only after the DHCP client function is enabled on the interface and an IP address is obtained.

Example

Renew the IP address lease on VLANIF100.

```
<Huawei> system-view
[Huawei] interface vlanif 100
[Huawei-Vlanif100] dhcp client renew
```

8.3.16 dhcp client request option-list exclude

Function

The **dhcp client request option-list exclude** command configures a list of default request options that are not carried in the Option55 field of DHCP Request messages.

The **undo dhcp client request option-list exclude** command deletes the list of default request options that are not carried in the Option55 field of DHCP Request messages.

 Copyright © Huawei Technologies Co., Ltd.

By default, the Option55 field in DHCP Request messages carries request options 3, 6, 15, 28, 33, 44, 121, and 184 by default.

Format

dhcp client request option-list exclude *option-code* &<1-8>

undo dhcp client request option-list exclude *option-code* &<1-8>

Parameters

Parameter	Description	Value
option-code	Specifies a list of default request options that are excluded from the Option55 field.	The value is of enumerated type and can be 3, 6, 15, 28, 33, 44, 121, and 184.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The Option55 field in DHCP Request messages is used to set the request option list. DHCP clients use this option to specify network configuration parameters that need to be obtained from the DHCP server. By default, the Option55 field carries request options 3, 6, 15, 28, 33, 44, 121, and 184 by default. You can run the **dhcp client request option-list exclude** command to configure a list of default options that are excluded from the Option55 field based on network requirements.

For option meanings, see *DHCP Options* in *CLI-based Configuration - IP Service Configuration Guide - DHCP Configuration*.

Example

Configure the default request option 3 to be excluded from the Option55 field in DHCP Request messages on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcp client request option-list exclude 3
```

 Copyright © Huawei Technologies Co., Ltd.

8.3.17 dhcp client request option-list

Function

The **dhcp client request option-list** command configures a list of request options that the Option55 field in DHCP Request packets carries besides the default options.

The **undo dhcp client request option-list** command deletes a list of request options that the Option55 field in DHCP Request packets carries besides the default options.

By default, the Option55 field in DHCP Request packets carries request options 3, 6, 15, 28, 33, 44, 121, and 184 by default.

Format

dhcp client request option-list *option-code* &<1-9>

undo dhcp client request option-list *option-code* &<1-9>

Parameters

Parameter	Description	Value
option-code	Specifies a list of request options that the Option55 field carries besides the default options.	The value is of enumerated type and can be 4, 7, 17, 42, 43, 66, 67, 120, and 129.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The Option55 field in DHCP Request packets is used to set the request option list. DHCP clients use this option to specify network configuration parameters that need to be obtained from the DHCP server. By default, the Option55 field carries request options 3, 6, 15, 28, 33, 44, 121, and 184 by default. Besides the default options, you can run the **dhcp client request option-list option-code** command to set a list of other request options that the Option55 field carries.

For option meanings, see *DHCP Options* in *CLI-based Configuration - IP Service Configuration Guide - DHCP Configuration*.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the Option55 field in DHCP Request packets to carry option 4 on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcp client request option-list 4
```

8.3.18 dhcp enable

Function

The **dhcp enable** command enables the DHCP function.

The **undo dhcp enable** command disables the DHCP function.

By default, the DHCP function is disabled.

Format

dhcp enable

undo dhcp enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Network scale and complexity increase makes network configurations complex. For example, computers frequently change their locations, and IP addresses are insufficient for these computers. The DHCP protocol is developed to address these problems. The **dhcp enable** command enables the DHCP function on the device.

Precautions

The **dhcp enable** command is the prerequisite for configuring DHCP-related functions, including DHCP relay, DHCP snooping, and DHCP server. These functions take effect only after the **dhcp enable** command is run. After the **undo dhcp enable** command is run, all DHCP-related configurations of the device are deleted. After DHCP is enabled again using the **dhcp enable** command, all DHCP-related configurations of the device are restored to the default configurations.

Follow-up Procedure

 Copyright © Huawei Technologies Co., Ltd.

Configure DHCP relay, DHCP Client, and DHCP server functions.

Example

Enable the DHCP function on the device.

```
<Huawei> system-view
[Huawei] dhcp enable
```

Related Topics

8.3.26 dhcp select interface

8.3.75 dns-list

8.3.19 dhcp link arp

Function

The **dhcp link arp** command configures an interface of a DHCP client to deliver a static ARP entry after it receives a DHCP ACK packet from the DHCP server.

The **undo dhcp link arp** command configures an interface of a DHCP client not to deliver a static ARP entry after it receives a DHCP ACK packet from the DHCP server.

By default, an interface of a DHCP client does not deliver a static ARP entry after it receives a DHCP ACK packet from the DHCP server.

Format

dhcp link arp

undo dhcp link arp

Parameters

None

Views

Ethernet interface view, Eth-Trunk interface view, GE interface view, VE interface view

Default Level

2: Configuration level

Usage Guidelines

You can use this command to configure a DHCP client to deliver a static ARP entry after it receives a DHCP ACK packet from the DHCP server.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure an interface of a DHCP client to deliver a static ARP entry after it receives a DHCP ACK packet from the DHCP server.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcp link arp
```

8.3.20 dhcp option template

Function

The **dhcp option template** command creates a DHCP Option template and enters the DHCP Option template view.

The **undo dhcp option template** command deletes a configured DHCP Option template.

By default, no DHCP Option template is created on the device.

Format

dhcp option template *template-name*

undo dhcp option template *template-name*

Parameters

Parameter	Description	Value
template-name	Specifies the name of the DHCP Option template.	The value is a string of 1 to 31 case-sensitive characters without spaces. The value can contain digits, letters, underscores (_), hyphens (-), and dots (.), but cannot be set to - or --.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on a DHCP server. During network deployment, a DHCP server dynamically allocates IP addresses with leases to clients or allocates fixed IP

 Copyright © Huawei Technologies Co., Ltd.

addresses to some clients. For example, laptops or terminals are often moved to different places in enterprises, and they can obtain IP addresses using the dynamic allocation mode. However, IP addresses obtained dynamically are randomly allocated, and cannot be set to specified IP addresses. To allocate fixed IP addresses to some fixed terminals (such as IP phones), run the **8.3.108 static-bind** command in the global address view to bind IP addresses to MAC addresses of the clients so that the clients are allocated fixed IP addresses.

In some cases, you need to allocate other network configuration parameters except IP addresses to fixed static terminals. For example, besides obtaining an IP address, an IP phone needs information such as the startup configuration file to register normally. In this case, you can configure a DHCP Option template and configure network configuration parameters except the IP address required by the client in the DHCP Option template. Then bind the DHCP Option template to the fixed terminal in the global address pool. The DHCP server then allocates the IP address and other parameters to the terminal.

Precautions

Network parameters configured in the DHCP Option template view take effect only for static clients. A DHCP Option template can be bound to multiple clients. Run the **static-bind ip-address** *ip-address* **mac-address** *mac-address* [**option-template** *template-name*] command to configure a DHCP Option template that is bound to static clients.

Example

Create a DHCP Option template named **test**.

```
<Huawei> system-view
[Huawei] dhcp option template test
```

Related Topics

8.3.64 display dhcp option template

8.3.108 static-bind

8.3.21 dhcp relay release

Function

The **dhcp relay release** command configures a DHCP relay agent to send a release message to a DHCP server for releasing the IP address assigned to a DHCP client.

Format

In the system view:

dhcp relay release *client-ip-address mac-address* [**vpn-instance** *vpn-instance-name*] [*server-ip-address*]

In the interface view:

dhcp relay release *client-ip-address mac-address* [*server-ip-address*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
client-ip-address	Specifies the IP address of a DHCP client.	The value is in dotted decimal notation.
mac-address	Specifies the MAC address of a DHCP client.	The value is in H-H-H format. H is a hexadecimal number of 1 to 4 digits.
server-ip-address	Specifies the IP address of a DHCP server. If this parameter is specified, a DHCP relay agent sends a release message to the specified DHCP server for releasing the IP address assigned to a DHCP client.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance to which the specified DHCP server releasing IP addresses belongs.	The value must an existing VPN name.

Views

Interface view, system view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP relay agents. In some situations, for example, a user is forced to go offline, the user's IP address is no longer used. However, the user cannot access the network, and will not send a DHCP release message to the DHCP server to release the IP address assigned by the DHCP server. Before the IP address lease expires, the DHCP server will not assign the user's IP address to another client, wasting IP addresses. In this case, you can run the **dhcp relay release** command to configure a DHCP relay agent to send a DHCP release message to the DHCP server. After receiving the message, the DHCP server sets the status of the IP address to idle. The DHCP server then can assign the released IP address to another client.

If a DHCP server address is specified, the DHCP relay agent sends an address release request only to the specified DHCP server. If no DHCP server address is specified, the following situations occur:

 Copyright © Huawei Technologies Co., Ltd.

- When the **dhcp relay release** command is run in the system view, the DHCP relay agent sends an address release request to DHCP servers on all the interfaces working in DHCP relay mode.
- When the **dhcp relay release** command is run in the interface view, the DHCP relay agent sends an address release request to all DHCP servers on the VLANIF interface.

Precautions

The **dhcp relay release** command only releases the IP addresses dynamically assigned by DHCP servers.

Example

Configure a DHCP relay agent to send a release message to the DHCP server at 10.1.1.1 for releasing the IP address 192.168.1.1 assigned to the DHCP client whose MAC address is 0050-ba34-2000.

```
<Huawei> system-view
[Huawei] dhcp relay release 192.168.1.1 0050-ba34-2000 10.1.1.1
```

8.3.22 dhcp relay server-ip

Function

The **dhcp relay server-ip** command configures a DHCP server address on an interface enabled with DHCP relay.

The **undo dhcp relay server-ip** command deletes the configured DHCP server addresses on an interface enabled with DHCP relay.

By default, no DHCP server address on an interface enabled with DHCP relay is configured.

Format

dhcp relay server-ip *ip-address*

undo dhcp relay server-ip { *ip-address* | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a DHCP server.	The value is in dotted decimal notation.
all	Deletes all the DHCP server addresses configured on an interface.	-

Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP relay agents. When a DHCP client needs to send a DHCP Discover message to a DHCP server on a different network segment through a DHCP relay agent, you must configure the DHCP server address on the DHCP relay agent.

When a DHCP relay agent forwards a DHCP Discover message, it does not check whether the DHCP server status is Down. If multiple DHCP server addresses are configured on an interface, multiple DHCP servers respond with DHCP Offer messages to the DHCP client. However, the DHCP client uses the first received DHCP Offer message. As a result, IP addresses in the IP address pool on the first DHCP server are insufficient, but available IP addresses in the IP address pools on the other DHCP servers are not allocated. To make each DHCP server allocate the same number of IP addresses, a DHCP relay agent changes the forwarding order each time it forwards a DHCP Discover message, so that load balancing is implemented among DHCP servers. A DHCP relay agent forwards a DHCP Discover message as follows:

- The DHCP relay agent forwards the message to all DHCP servers by default, and changes the forwarding order each time it forwards a DHCP Discover message.
- You can configure the **8.3.85 ip relay address cycle** command to reduce the number of packets received by a DHCP server and lessen the load of a DHCP server. After this command is configured, the DHCP relay agent forwards a received DHCP Discover message to one DHCP server at a time, and forwards the DHCP Discover message to a different DHCP server each time it receives the message.

Prerequisites

DHCP relay has been enabled on the interface using the **dhcp select relay** command.

Precautions

If you run the **dhcp relay server-ip** command for multiple times, multiple DHCP server addresses are configured.

Each interface that is enabled with DHCP relay can be configured with a maximum of 8 DHCP server addresses.

Example

Configure DHCP relay on GE1/0/0 and add two DHCP server addresses.

```
<Huawei> system-view
[Huawei] dhcp enable
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcp select relay
[Huawei-GigabitEthernet1/0/0] dhcp relay server-ip 10.1.1.2
[Huawei-GigabitEthernet1/0/0] dhcp relay server-ip 10.1.1.3
```

Related Topics

8.3.28 dhcp select relay

8.3.23 dhcp relay server-select

Function

The **dhcp relay server-select** command configures a DHCP server group for a DHCP relay agent.

The **undo dhcp relay server-select** command deletes the configured DHCP server group of a DHCP relay agent.

By default, no DHCP server group is configured.

Format

dhcp relay server-select *group-name*

undo dhcp relay server-select

Parameters

Parameter	Description	Value
group-name	Specifies the name of a DHCP server group.	The value is a string of 1 to 32 case-sensitive characters without spaces.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp relay server-select** command applies to DHCP relay agents. When a DHCP client needs to send DHCP requests to a DHCP server using a DHCP relay agent, you can run the **dhcp relay server-select** command to specify a DHCP server group for the DHCP relay agent and configure the DHCP server address.

Prerequisites

Copyright © Huawei Technologies Co., Ltd.

1. A DHCP server group has been created using the **dhcp server group** command.
2. The DHCP relay function has been enabled using the **dhcp select relay** command so that the system can forward DHCP packets to the specified DHCP server.

Precautions

- Multiple interfaces can be configured with the same DHCP server group, and one interface can be configured with only one DHCP server group.
- Addresses of DHCP servers in a DHCP server group cannot be on the same network segment with addresses of interfaces enabled with DHCP relay.
- If you run the **dhcp relay server-select** command in the same interface view for multiple times, only the latest configuration takes effect. If a specified DHCP server group does not exist, the configuration fails; however, the latest configured DHCP server group still takes effect.
- The **dhcp relay server-select** command can only be used on Layer 3 interfaces, including Layer 3 GE interfaces, Layer 3 Ethernet interfaces, and Layer 3 Eth-Trunk interfaces.

Example

Configure the DHCP server group of a DHCP relay agent as **group1** on GE1/0/0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp server group group1
[Huawei-dhcp-server-group-group1] dhcp-server 10.10.10.10
[Huawei-dhcp-server-group-group1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcp select relay
[Huawei-GigabitEthernet1/0/0] dhcp relay server-select group1
```

Related Topics

8.3.40 dhcp server group
8.3.59 dhcp-server
8.3.65 display dhcp relay

8.3.24 dhcp relay trust option82

Function

The **dhcp relay trust option82** command enables Option 82 on the DHCP relay agent.

The **undo dhcp relay trust option82** command disables Option 82 on the DHCP relay agent.

By default, Option 82 is enabled on the DHCP relay agent.

Format

dhcp relay trust option82

undo dhcp relay trust option82

Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on the DHCP relay agent to enable the Option 82 function. After receiving a DHCP packet that carries the Option 82 field but the giaddr field of the packet is 0, the DHCP relay agent processes the packet by default. Using the **undo dhcp relay trust option82** command, the DHCP relay agent discards the packet.

Prerequisites

DHCP has been enabled globally by using the **dhcp enable** command.

Example

Enable Option 82 trusted of the DHCP relay agent.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp relay trust option82
```

8.3.25 dhcp select global

Function

The **dhcp select global** command enables an interface to use the global address pool.

The **undo dhcp select global** command disables an interface from using the global address pool.

By default, an interface is disabled from using the global address pool.

Format

dhcp select global

undo dhcp select global

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp select global** command applies to DHCP servers. After receiving a DHCP Request message from a DHCP client, a DHCP server assigns an IP address from the local address pool to the client. Run the **dhcp select global** command to configure the device to assign IP addresses from the global address pool. When no interface address pool is created for the DHCP server, the DHCP server assigns an IP address from the global address pool to an online user.

The device can also assign IP addresses from an interface address pool using the **dhcp select interface** command in the interface view.

Prerequisites

- DHCP has been enabled using the **dhcp enable** command in the system view.
- Before running the **dhcp select global** command, you need to run the **ip address** command to configure the interface IP address.

Precautions

- When the device is configured as a DHCP server, if the server's real IP address is configured as the DHCP server IP address on a DHCP relay agent, the server's Layer 3 interface that receives relayed DHCP messages can process these messages, without the need of running the **dhcp select global** command on the interface.
- When the device is configured as a DHCP server, if the VRRP virtual IP address of the server's Layer 3 interface that does not receive DHCP messages is configured as the DHCP server IP address on the DHCP relay agent, the DHCP server cannot process messages relayed by the DHCP relay agent. The DHCP server can process messages relayed by the DHCP relay agent only if the VRRP virtual IP address of the server's Layer 3 interface that receives DHCP messages is configured as the DHCP server IP address on the DHCP relay agent and the **dhcp select global** command is configured on this Layer 3 interface.
- In IPoEoA scenarios, the DHCP server function for the global address pool cannot be enabled on a VE interface of a device. That is, the **dhcp select global** and **map bridge virtual-ethernet** *interface-number* commands cannot be configured on the same VE interface. Otherwise, the DHCP server function does not take effect.

Example

Enable GE1/0/0 to use the global address pool.

```
<Huawei> system-view
[Huawei] dhcp enable
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[Huawei-GigabitEthernet1/0/0] dhcp select global
```

Related Topics

8.3.18 dhcp enable

8.3.83 ip pool (system view)

8.3.26 dhcp select interface

7.5.13 map bridge

8.3.26 dhcp select interface

Function

The **dhcp select interface** command enables an interface to use the interface address pool.

The **undo dhcp select interface** command disables an interface from using the interface address pool.

By default, the DHCP server function using the interface address pool is disabled on an interface.

Format

dhcp select interface

undo dhcp select interface

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp select interface** command applies to DHCP servers. After receiving a DHCP Request message from a DHCP client, a DHCP server assigns an IP address from the local address pool to the client. Run the **dhcp select interface** command to configure a DHCP server to assign IP addresses from the interface address pool to clients.

The device can also assign IP addresses from a global address pool using the **dhcp select global** command.

Copyright © Huawei Technologies Co., Ltd.

NOTE

This command is not supported in the tunnel interface view.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command in the system view.

An IP address has been configured for an interface using the **ip address** command. The IP addresses assigned by the address pool and configured on the interface are on the same network segment.

Precautions

- By default, an management interface is disabled from the DHCP server function using the interface address pool. However, the **dhcp select interface** command is added to the factory settings of an management interface. In this way, when a device is started based on the factory settings, the DHCP server function of the management interface is enabled.
- In IPoEoA scenarios, the DHCP server function for the interface address pool cannot be enabled on a VE interface of a device. That is, the **dhcp select interface** and **map bridge virtual-ethernet** *interface-number* commands cannot be configured on the same VE interface. Otherwise, the DHCP server function does not take effect.

Example

Enable GE1/0/0 to use the interface address pool.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.1.1.2 24
[Huawei-GigabitEthernet1/0/0] dhcp select interface
```

Related Topics

7.5.13 map bridge

8.3.27 dhcp server alarm ip-used percentage

Function

The **dhcp server alarm ip-used percentage** command configures the percentage of the alarms indicating that the addresses in an interface address pool are used up, and the percentage of the clear alarms.

The **undo dhcp server alarm ip-used percentage** command restores the default percentages of the alarms and clear alarms.

By default, the percentage of the alarms indicating that the addresses in an interface address pool are used up is 100%, and the percentage of the clear alarms is 50%.

Format

dhcp server alarm ip-used percentage *alarm-resume-percentage alarm-percentage*

Copyright © Huawei Technologies Co., Ltd.

undo dhcp server alarm ip-used percentage

Parameters

Parameter	Description	Value
alarm-resume-percentage	Specifies the percentage of the clear alarms.	The value is an integer that ranges from 1 to 100. The default value is **50**. **NOTE** The percentage of the clear alarms cannot exceed that of the alarms.
alarm-percentage	Specifies the percentage of the alarms indicating that the addresses in an address pool are used up.	The value is an integer that ranges from 1 to 100. The default value is **100**.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the addresses in an interface address pool are used up, alarms are sent to notify the administrator.

Precautions

The percentage of the clear alarms cannot exceed that of the alarms.

Example

Configure the percentage of the alarms indicating that the addresses in an interface address pool are used up, and the percentage of the clear alarms in the interface address pool of the VLANIF100.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface vlanif 100
[Huawei-Vlanif100] ip address 10.10.10.10 24
[Huawei-Vlanif100] dhcp select interface
[Huawei-Vlanif100] dhcp server alarm ip-used percentage 80 90
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

8.3.18 dhcp enable

8.3.26 dhcp select interface

8.3.28 dhcp select relay

Function

The **dhcp select relay** command enables the DHCP relay function.

The **undo dhcp select relay** command disables the DHCP relay function.

By default, the DHCP relay function is disabled.

Format

dhcp select relay

undo dhcp select relay

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp select relay** command applies to DHCP relay agents. If the DHCP server and client are on the same network segment, they can directly communicate with each other using DHCP. In this case, no DHCP relay agent is needed. If the DHCP server and client are on different network segments, the DHCP relay function must be enabled to forward DHCP messages.

Prerequisites

The DHCP function has been enabled using the **8.3.18 dhcp enable** command in the system view.

Follow-up Tasks

- To ensure that a DHCP relay agent can forward DHCP packets to a DHCP server, run the **8.3.23 dhcp relay server-select** or **dhcp relay server-ip** command on the DHCP relay-enabled interface to configure the correct IP address of the DHCP server.

 Copyright © Huawei Technologies Co., Ltd.

- To ensure that a DHCP server can forward DHCP packets to a DHCP relay agent, you must configure a route to the DHCP relay agent on the DHCP server.

Precautions

- The DHCP server must select an IP address in the same network segment with the DHCP relay agent from the global address pool to ensure that the DHCP client obtains an IP address on the local network segment. No interface address pool can be configured on the interface that connects the DHCP server and relay agent.
- Before using the **dhcp select relay** command on a G.SHDSL or VDSL interface, ensure that the interface works in PTM mode.
- If DHCP relay is enabled in a super-VLAN, DHCP snooping cannot be enabled in this super-VLAN.

Example

Enable the DHCP relay function on GE1/0/0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcp select relay
```

Related Topics

8.3.23 dhcp relay server-select

8.3.22 dhcp relay server-ip

8.3.29 dhcp server bootfile

Function

The **dhcp server bootfile** command configures the name of the startup configuration file for a DHCP client.

The **undo dhcp server bootfile** command deletes the configured name of the startup configuration file for a DHCP client.

By default, the startup configuration file name is not configured for a DHCP client.

Format

dhcp server bootfile *bootfile*

undo dhcp server bootfile

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
bootfile	Specifies the name of the startup configuration file for a DHCP client.	The value is a string of 1 to 127 case-sensitive characters without spaces.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Besides assigning IP addresses, a DHCP server can also provide the required network configuration parameters, such as the startup configuration file name for the DHCP clients. After the name of the startup configuration file is configured using the **dhcp server bootfile** command, the Offer and ACK packets sent from the DHCP server carry this file name. The DHCP client can acquire the startup configuration file from the specified server based on the file name.

Prerequisites

1. The DHCP function has been enabled using the **8.3.18 dhcp enable** command in the system view.
2. The DHCP server has been enabled on the interface using the **8.3.26 dhcp select interface** command.

Example

Configure the name of the startup configuration file as **start.ini** for the DHCP client on the Vlanif100.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface vlanif 100
[Huawei-Vlanif100] ip address 192.168.1.1 255.255.255.0
[Huawei-Vlanif100] dhcp select interface
[Huawei-Vlanif100] dhcp server bootfile start.ini
```

Related Topics

8.3.18 dhcp enable

8.3.26 dhcp select interface

Copyright © Huawei Technologies Co., Ltd.

8.3.30 dhcp server bootp

Function

Using the **dhcp server bootp** command, you can enable a DHCP server to respond to a Bootstrap Protocol (BOOTP) request.

Using the **undo dhcp server bootp** command, you can disable a DHCP server from responding to a BOOTP request.

By default, a DHCP server responds to a BOOTP request.

Format

dhcp server bootp

undo dhcp server bootp

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A DHCP server and a BOOTP server may reside on the same network segment. The BOOTP server assigns static IP addresses to BOOTP clients. As defined in the DHCP protocol, a DHCP server can also respond to BOOTP requests to assign IP addresses to BOOTP clients. BOOTP clients may obtain IP addresses from the DHCP server but not the BOOTP server.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command in the system view.

Follow-up Procedure

Using the **dhcp server bootp automatic** command in the system view, you can enable the DHCP server to allocate IP addresses to BOOTP clients.

Example

Enable a DHCP server to respond to a BOOTP request.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp server bootp
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

8.3.18 dhcp enable

8.3.31 dhcp server bootp automatic

Function

The **dhcp server bootp automatic** command enables the DHCP server to dynamically allocate IP addresses to BOOTP clients.

The **undo dhcp server bootp automatic** command disables the DHCP server from dynamically allocating IP addresses to BOOTP clients.

By default, a DHCP server does not dynamically allocate IP addresses to BOOTP clients.

Format

dhcp server bootp automatic

undo dhcp server bootp automatic

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. When BOOTP clients need to obtain their IP addresses, DNS server's IP address, and gateway IP address from a DHCP server, you need to run the **dhcp server bootp automatic** command to enable the DHCP server to dynamically allocate IP addresses to BOOTP clients.

Prerequisites

- DHCP has been enabled globally using the **dhcp enable** command in the system view.
- The DHCP server has been enabled to respond to BOOTP requests by using the **dhcp server bootp** command, or **dhcp server bootp automatic** cannot take effect.

Precautions

When the device functions as the DHCP server, the device can allocate IP addresses to BOOTP clients if the BOOTP clients reside on the same network as

 Copyright © Huawei Technologies Co., Ltd.

the DHCP server. You can run the **dhcp server bootp automatic** command to dynamically allocate IP addresses. You can also run the **static-bind** command or the **dhcp server static-bind** command to allocate IP addresses to BOOTP clients in the static binding mode.

Example

Enable the DHCP server to allocate IP addresses to BOOTP clients.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp server bootp
[Huawei] dhcp server bootp automatic
```

Related Topics

8.3.18 dhcp enable

8.3.30 dhcp server bootp

8.3.32 dhcp server conflict auto-recycle interval

Function

The **dhcp server conflict auto-recycle interval** command enables automatic reclaim of conflicting IP addresses in the interface address pool and configures the interval for the automatic reclaim.

The **undo dhcp server conflict auto-recycle interval** command disables automatic reclaim of conflicting IP addresses in the interface address pool and deletes the configured interval for the automatic reclaim.

By default, automatic reclaim of conflicting IP addresses in the interface address pool is disabled.

Format

dhcp server conflict auto-recycle interval day *day* [**hour** *hour* [**minute** *minute*]]

undo dhcp server conflict auto-recycle interval

Parameters

Parameter	Description	Value
day *day*	Specifies the interval for the automatic reclaim, in days.	The value is an integer that ranges from 0 to 999, in days. The default value is 0.
hour *hour*	Specifies the interval for the automatic reclaim, in hours.	The value is an integer that ranges from 0 to 23, in hours. The default value is 0.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
minute *minute*	Specifies the interval for the automatic reclaim, in minutes.	The value is an integer that ranges from 0 to 59, in minutes. The default value is 0.

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on a DHCP server. When a DHCP server allocates IP addresses to clients, IP address conflict may occur because IP addresses of some hosts have been manually configured. In this case, the DHCP server considers these IP addresses as conflicting IP addresses, and allocates available IP addresses from the conflicting IP addresses to clients only after available IP addresses in the address pool are used up. To reclaim conflicting IP addresses promptly, the administrator can run this command to enable automatic reclaim and specify the reclaim interval.

Prerequisites

1. IP addresses in the interface address pool have been configured using the **ip address** command.
2. The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Example

Enable automatic reclaim for conflicting IP addresses in the address pool on VLANIF 100, and set the interval for automatic reclaim to one day.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface vlanif 100
[Huawei-Vlanif100] ip address 192.168.1.1 24
[Huawei-Vlanif100] dhcp select interface
[Huawei-Vlanif100] dhcp server conflict auto-recycle interval day 1
```

8.3.33 dhcp server database

Function

The **dhcp server database** command enables the function to save the current DHCP data to storage devices.

Copyright © Huawei Technologies Co., Ltd.

The **undo dhcp server database** command disables the function to save the DHCP data to storage devices.

By default, DHCP data is not saved to storage devices.

Format

dhcp server database { **enable** | **recover** | **write-delay** *interval* }

undo dhcp server database { **enable** | **recover** | **write-delay** }

Parameters

Parameter	Description	Value
enable	Enables the function to save DHCP data to storage devices.	-
recover	Recovers DHCP configurations using DHCP data in storage device.	-
write-delay *interval*	Specifies the interval at which DHCP data is saved.	The value is an integer ranging from 300 to 86400, in seconds. The default value is 3600 seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device functions as a DHCP server, run the **dhcp server database enable** command to enable the device to save DHCP data to storage devices. This avoids data loss caused by device faults. Then the system generates **lease.txt** and **conflict.txt** files in the storage device. The two files save address lease information and address conflict information respectively. Run the **8.3.67 display dhcp server database** command to check the storage device for saving DHCP data. After the **dhcp server database enable** command is run, current DHCP data is automatically saved at the specified interval, and previous data files are overwritten. The interval can be set using the **dhcp server database write-delay** *interval* command.

Copyright © Huawei Technologies Co., Ltd.

If a fault occurs on the device, run the **dhcp server database recover** command to recover DHCP data from storage devices during the system restarts.

Prerequisites

The **dhcp server database enable** command has been run to enable the device to save DHCP data to storage devices, and ensure that the storage devices work properly.

Precautions

- The lease.txt and conflict.txt files are overwritten periodically; therefore, you are advised to back up and save the two files to other locations.
- The time displayed in the lease.txt and conflict.txt files is the UTC time rather than the system time, and you do not need to pay attention to time zone information.

Example

Enable the device to save the current DHCP data to storage devices and set the interval at which DHCP data is saved to 2000s.

```
<Huawei> system-view
[Huawei] dhcp server database enable
[Huawei] dhcp server database write-delay 2000
```

Recover DHCP configuration using the DHCP data saved on storage devices.

```
<Huawei> system-view
[Huawei] dhcp server database recover
```

Related Topics

8.3.67 display dhcp server database

8.3.34 dhcp server dns-list

Function

The **dhcp server dns-list** command configures DNS server addresses for an interface address pool.

The **undo dhcp server dns-list** command deletes the specified DNS server addresses of an interface address pool.

By default, no DNS server address is configured in an interface address pool.

Format

dhcp server dns-list { *ip-address* &<1-8> | **unnumbered interface** *interface-type interface-number* }

undo dhcp server dns-list { **all** | *ip-address* | **unnumbered interface** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of the DNS server. You can configure up to eight IP addresses for the DNS servers and separate two IP addresses with a space.	The value is in dotted decimal notation.
unnumbered interface *interface-type interface-number*	Borrows the DNS server address obtained by the interface as the DNS server IP address.	-
all	Deletes all IP addresses of DNS servers specified for the client.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. If user hosts access hosts on the network through the domain name, user hosts need to send DNS Request messages to the DNS server and resolve the domain name. To enable DNS services on the DHCP client, specify the DNS server address for the interface address pool on the DHCP server. The DHCP server can assign both the specified DHCP server address and an IP address to the client. To configure DNS server addresses for a global address pool, run the **dns-list** command.

Prerequisites

- The address of an interface address pool has been configured using the **ip address** command.
- The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Precautions

- Each address pool can be configured with a maximum of eight DNS server addresses. If multiple DNS server addresses are configured, the first DNS server address assigned to the DHCP client functions as the primary address and other addresses are secondary addresses.
- To specify multiple DNS servers, enter multiple DNS server addresses in the **dhcp server dns-list** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Specify a DNS server at 10.10.1.254 for domain name resolution when IP addresses in the interface address pool on GE1/0/0 are assigned to clients.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server dns-list 10.10.1.254
```

Related Topics

8.3.26 dhcp select interface

8.3.75 dns-list

8.3.35 dhcp server domain-name (interface view)

8.3.35 dhcp server domain-name (interface view)

Function

The **dhcp server domain-name** command configures a DNS domain name assigned to a DHCP client.

The **undo dhcp server domain-name** command deletes a specified domain name.

By default, no domain name is configured for the DHCP client.

Format

dhcp server domain-name *domain-name*

undo dhcp server domain-name

Parameters

Parameter	Description	Value
domain-name	Specifies the domain name that the DHCP server assigns to the client.	The value is a string of 1 to 63 characters without spaces. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.

Views

Interface view

Default Level

2: Configuration level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. Run the **dhcp server domain-name** command on a DHCP server to specify a domain name for each interface address pool. When allocating IP addresses to clients, the DHCP server also sends the domain names to the clients.

Prerequisites

- The address of an interface address pool has been configured using the **ip address** command.
- The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Precautions

To configure a domain name for the global address pool, run the **domain-name** command.

Example

Set the domain name assigned by the DHCP address pool on the interface to **example.com**.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server domain-name example.com
```

Related Topics

8.3.76 domain-name

8.3.26 dhcp select interface

8.3.36 dhcp server excluded-ip-address

Function

The **dhcp server excluded-ip-address** command specifies the range of IP addresses that cannot be automatically assigned to clients from an interface address pool.

The **undo dhcp server excluded-ip-address** command deletes the specified range of IP addresses that cannot be automatically assigned to clients from the interface address pool.

By default, all IP addresses in the address pool can be automatically assigned to clients.

Format

dhcp server excluded-ip-address *start-ip-address* [*end-ip-address*]

undo dhcp server excluded-ip-address *start-ip-address* [*end-ip-address*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
start-ip-address	Specifies the start IP address that cannot be automatically assigned.	The value is in dotted decimal notation.
end-ip-address	Specifies the end IP address that cannot be automatically assigned. If *end-ip-address* is not specified, only *start-ip-address* cannot be automatically assigned.	The value is in dotted decimal notation. *end-ip-address* and *start-ip-address* must be on the same network segment and *end-ip-address* must be larger than *start-ip-address*.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp server excluded-ip-address** command applies to DHCP servers. Fixed IP addresses are allocated to some specific hosts (such as the WWW server) on the network for a long time. If these hosts' IP addresses are overlapped with IP addresses in the address pool and the DHCP server allocates these overlapped IP addresses to other hosts, IP address conflicts may occur. To prevent the IP address conflict, you need to exclude these IP addresses from being automatically allocated in the address pool.

You can run the **dhcp server excluded-ip-address** command to specify the IP addresses or the range of IP addresses that cannot be automatically assigned to clients in the interface address pool.

You can run the **excluded-ip-address** command to specify the IP addresses or the range of IP addresses that cannot be automatically assigned to clients in the global address pool.

Prerequisites

- An address segment in the interface address pool is configured using the **ip address** command.
- The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

- IP addresses that cannot be automatically assigned must be in the address pool. If the range of IP addresses in the address pool is changed using the **dhcp server ip-range** command, IP addresses that are configured not to be automatically assigned must be within the changed IP address range.
- You do not need to exclude the gateway address configured using the **8.3.37 dhcp server gateway-list** command from being automatically allocated. The device automatically adds the gateway address into the list of IP addresses that cannot be automatically allocated.

  You do not need to exclude the IP address of a server's interface connecting to a client from being automatically allocated. The device automatically sets the interface IP address to the Conflict status during address allocation.
- If you run this command multiple times, you can specify multiple IP addresses or IP address segments that cannot be automatically assigned to clients from the specified address pool.
- You can run the **display ip pool** command to check used IP addresses in the current address pool, and then specify unused IP addresses that cannot be automatically assigned. To exclude used IP addresses from being automatically assigned, run the **reset ip pool** command to reclaim used IP addresses first.

Example

Specify that IP addresses 192.168.1.1 to 192.168.1.20 cannot be automatically assigned to clients from the address pool on GE1/0/0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 192.168.1.1 24
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server excluded-ip-address 192.168.1.1 192.168.1.20
```

Related Topics

8.3.26 dhcp select interface

8.3.77 excluded-ip-address

8.3.37 dhcp server gateway-list

Function

The **dhcp server gateway-list** command sets the default gateway IP address that a DHCP server pre-allocates to DHCP clients.

The **undo dhcp server gateway-list** command deletes the configured default gateway IP address.

By default, the default gateway IP address that a DHCP server pre-allocates to DHCP clients is not configured.

Format

dhcp server gateway-list *ip-address* &<1-8>

undo dhcp server gateway-list { *ip-address* | **all** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip-address	Specifies an IP address. You can configure a maximum of eight gateway addresses, which are separated by spaces.	The value is in decimal dotted notation.
all	Indicates all IP addresses.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

To load balance traffic and improve network reliability, you can configure multiple default gateway addresses.

NOTICE

Do not configure the default gateway address allocated to DHCP clients as a broadcast address.

If the VRRP virtual IP address is configured on the interface and no gateway address is pre-allocated to the DHCP client using the **dhcp server gateway-list** command, the DHCP server uses the first VRRP virtual IP address as the gateway address to be allocated to the client. If no VRRP virtual IP address is configured on the interface, the DHCP server uses the physical IP address of the interface as the gateway address to be allocated to the client.

If the **dhcp server gateway-list** command is not configured, the gateway address allocated by the DHCP server to the DHCP client may fail to be displayed in trace information during fault diagnosis. Therefore, you are advised to configure this command if the DHCP server function based on an interface address pool is used.

Example

Enable a DHCP server on a GE1/0/0 to pre-allocate default gateway address 10.1.1.1 to DHCP clients.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server gateway-list 10.1.1.1
```

8.3.38 dhcp server force insert option

Copyright © Huawei Technologies Co., Ltd.

Function

The **dhcp server force insert option** command configures a DHCP server to forcibly insert an Option field specified in the interface address pool to a DHCP Response packet that it sends to a DHCP client.

The **undo dhcp server force insert option** command deletes the Option field forcibly inserted to a DHCP Response packet that a DHCP server sends to a DHCP client.

By default, a DHCP server does not forcibly insert an Option field to a DHCP Response packet that it sends to a DHCP client.

Format

dhcp server force insert option *code* &<1-254>

undo dhcp server force insert option *code* &<1-254>

Parameters

Parameter	Description	Value
code	Specifies the code for a forcibly replied option. You can configure a DHCP server to forcibly reply one or more options.	The value is an integer that ranges from 1 to 254.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In general, when a DHCP client applies for an IP address from a DHCP server, parameters contained in the DHCP Request packet specify the options the client requires. The DHCP server inserts the required options to a DHCP Response packet.

Sometimes, a device, functioning as a DHCP server, receives a DHCP Request packet that contains no parameter specifying the options the client requires. However, the client still wants to obtain the options configured on the interface address pool. You can run the **dhcp server force insert option** *code* &<1-254> command to configure the DHCP server to forcibly insert an Option field to the DHCP Response packet.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

1. The device has been configured to assign IP addresses in the interface address pool using the **dhcp select interface** command.
2. The Option field has been configured in the interface address pool using the **dhcp server option** *code* [**sub-option** *sub-code*] { **ascii** *ascii-string* | **hex** *hex-string* | **cipher** *cipher-string* | **ip-address** *ip-address* &<1-8> } command in the interface view.

Example

Configure a DHCP server to forcibly insert Option 4 to a DHCP Response packet on GE1/0/0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server option 4 hex 11 22
[Huawei-GigabitEthernet1/0/0] dhcp server force insert option 4
```

Related Topics

8.3.26 dhcp select interface

8.3.49 dhcp server option

8.3.39 dhcp server force response

Function

The **dhcp server force response** command forces a DHCP server to reply with a DHCP NAK message.

The **undo dhcp server force response** command restores the default settings.

By default, a DHCP server is not forced to reply with a DHCP NAK message.

Format

dhcp server force response

undo dhcp server force response

Parameters

None

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Scenario

When a DHCP client goes online in two steps, the IP address requested by the DHCP client is in the IP address pool, but no lease record of the DHCP client is found in the address pool. For example, after obtaining an IP address from another DHCP server, a wireless user roams to the current DHCP server and the original IP address is in the address pool of the current DHCP server. Alternatively, the address pool is reset and the original user needs to go online again. In this case, when receiving a DHCP Request message from the DHCP client, the DHCP server keeps silent and does not reply the DHCP client with a DHCP NAK message. The DHCP client can apply for an IP address to go online again in four steps only after the two steps for the client to go online time out. As a result, the DHCP client is slow in obtaining an IP address. To force the DHCP server to reply with a DHCP NAK message, you can run the **dhcp server force response** command, so that the DHCP client can quickly enter the four-step process for going online and apply for an IP address again.

Prerequisites

DHCP has been enabled on the device using the **dhcp enable** command.

Example

Force a DHCP server to reply with a DHCP NAK message.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp server force response
```

8.3.40 dhcp server group

Function

The **dhcp server group** command creates a DHCP server group and displays the DHCP server group view or directly displays the view of the existing DHCP server group.

The **undo dhcp server group** command deletes an existing DHCP server group.

By default, no DHCP server group is configured.

Format

dhcp server group *group-name*

undo dhcp server group *group-name*

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
group-name	Specifies the name of a DHCP server group.	The value is a string of 1 to 32 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP relay agents. Generally, a DHCP relay agent serves multiple DHCP servers. To manage these DHCP servers in a unified manner, run the **dhcp server group** command to create a DHCP server group. The DHCP server group then assigns IP addresses to users using the DHCP relay agent.

Follow-up Procedure

- Run the **dhcp-server** command to add DHCP servers to the DHCP server group.
- Run the **8.3.23 dhcp relay server-select** command in the interface view to specify a DHCP server group for the DHCP relay agent.

Precautions

You can configure a maximum of 64 DHCP server groups in the system, and a maximum of 8 DHCP servers in a DHCP server group.

Example

Create a DHCP server group named **dhcp-srv1**.

```
<Huawei> system-view
[Huawei] dhcp server group dhcp-srv1
```

Related Topics

8.3.59 dhcp-server

8.3.68 display dhcp server group

8.3.23 dhcp relay server-select

Copyright © Huawei Technologies Co., Ltd.

8.3.41 dhcp server import all

Function

The **dhcp server import all** command enables the device to automatically obtain the DNS server IP address, DNS domain name suffix, and NetBIOS server IP address from an interface address pool.

The **undo dhcp server import all** command disables the device from automatically obtaining the DNS server IP address, DNS domain name suffix, and NetBIOS server IP address from an interface address pool.

By default, the device is disabled from automatically obtaining the DNS server IP address, DNS domain name suffix, and NetBIOS server IP address from an interface address pool.

Format

dhcp server import all

undo dhcp server import all

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on the DHCP server. Run the **dhcp server import all** command on the DHCP server to automatically allocate the DNS server IP address, DNS domain name suffix, and NetBIOS server IP address from the carrier to the DHCP client.

Prerequisites

The DHCP server has been enabled on the interface using the **8.3.26 dhcp select interface** command.

Precautions

The **dhcp server import all** command can only be used on Layer 3 interfaces, including Layer 3 GE interfaces, Layer 3 Ethernet interfaces, and Layer 3 Eth-Trunk interfaces.

Copyright © Huawei Technologies Co., Ltd.

Example

Enable the device to automatically obtain configurations of the DNS server and NetBIOS server from an interface address pool.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server import all
```

Related Topics

8.3.72 display ip pool import all

8.3.102 reset ip pool import

8.3.42 dhcp server ip-range

Function

The **dhcp server ip-range** command sets the range of IP addresses that a DHCP server pre-allocates to DHCP clients.

The **undo dhcp server ip-range** command deletes the configured IP address range.

By default, the range of IP addresses that a DHCP server pre-allocates to DHCP clients is not configured.

Format

dhcp server ip-range *start-ip-address end-ip-address*

undo dhcp server ip-range

Parameters

Parameter	Description	Value
start-ip-address	Specifies the start IP address.	The value is in decimal dotted notation.
end-ip-address	Specifies the end IP address.	The value is in decimal dotted notation.

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Prerequisites

Usage Scenario

You can run the **dhcp server ip-range** *start-ip-address end-ip-address* command to change the range of IP addresses in an address pool based on actual usage of IP addresses.

Prerequisites

The DHCP server function of the interface address pool has been enabled on interfaces using the **dhcp select interface** command.

Example

Enable a DHCP server on a GE1/0/0 to pre-allocate IP addresses 192.168.1.2 to 192.168.1.100 to DHCP clients.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 192.168.1.1 24
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server ip-range 192.168.1.2 192.168.1.100
```

8.3.43 dhcp server lease

Function

The **dhcp server lease** command specifies the IP address lease for addresses in an interface address pool.

The **undo dhcp server lease** command restores the default IP address lease of addresses in an interface address pool.

By default, the IP address lease of addresses in an interface address pool is one day.

Format

dhcp server lease { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }

undo dhcp server lease

Parameters

Parameter	Description	Value
day *day*	Specifies the number of days in the IP address lease.	The value is an integer that ranges from 0 to 999. The default value is 1.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hour *hour*	Specifies the number of hours in the IP address lease.	The value is an integer that ranges from 0 to 23. The default value is 0.
minute *minute*	Specifies the number of minutes in the IP address lease.	The value is an integer that ranges from 0 to 59. The default value is 0.
unlimited	Indicates that the IP address lease is unlimited.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. To meet different client requirements, DHCP supports dynamic, automatic, and static address assignment.

DHCP clients require different IP address leases.

- If a host (such as the DNS server) needs to use a fixed IP address for a long time, run the **dhcp server lease unlimited** command to configure the IP address lease as unlimited.
- If a host (such as a portable computer) needs to use a temporary IP address, run the **dhcp server lease** command to specify an IP address lease. After the lease expires, the DHCP server withdraws the IP address and assigns the address to other clients.

When a DHCP client starts and 50% or 87.5% of its IP address lease has passed, the DHCP client sends a DHCP Request message to the DHCP server to renew the lease.

- If the IP address can still be assigned to the client, the DHCP server informs the client of a renewed IP address lease.
- If the IP address can no longer be assigned to the client, the DHCP server informs the client that the IP address lease cannot be renewed.

You can run the **8.3.71 display ip pool** command to view information about the IP address lease. The values of the **lease** and **left** fields in the command output indicate the configured lease time and remaining lease time, respectively.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

- The address of an interface address pool has been configured using the **ip address** command.
- The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Precautions

Different IP address leases can be specified for different interface address pools on a DHCP server. All IP addresses in an interface address pool have the same lease.

If the IP address lease of an address pool is changed using this command, newly assigned IP addresses use the new IP address lease. IP addresses assigned before the change still use the original IP address lease before the lease is updated, and use the new lease after the lease is updated.

Example

Set the IP address lease of the address pool on GE1/0/0 to 2 days 2 hours and 30 minutes.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.10.10.10 24
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server lease day 2 hour 2 minute 30
```

Related Topics

8.3.26 dhcp select interface

8.3.87 lease

8.3.44 dhcp server logging

Function

The **dhcp server logging** command enables the logging function during IP address allocation of the DHCP server in the interface view.

The **undo dhcp server logging** command disables the logging function during IP address allocation of the DHCP server in the interface view.

By default, the logging function during IP address allocation of the DHCP server is disabled.

Format

dhcp server logging [**allocation-fail** | **allocation-success** | **release** | **renew-fail** | **renew-success** | **detect-conflict** | **recycle-conflict**] *

undo dhcp server logging [**allocation-fail** | **allocation-success** | **release** | **renew-fail** | **renew-success** | **detect-conflict** | **recycle-conflict**] *

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
allocation-fail	Displays logs when address allocation fails.	-
allocation-success	Displays logs when address allocation succeeds.	-
release	Displays logs when addresses are released.	-
renew-fail	Displays logs when address lease renewal fails.	-
renew-success	Displays logs when address lease renewal succeeds.	-
detect-conflict	Displays logs when address conflict occurs.	-
recycle-conflict	Displays logs when conflicting addresses are reclaimed.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on a DHCP server. When the DHCP server allocates IP addresses to clients, it records address allocation information to facilitate routine maintenance and fault location. After the logging function during IP address allocation of the DHCP server is configured using the **dhcp server logging** command, the DHCP server records logs about address allocation, conflict, lease renewal, and release.

Run the **display ip pool** **interface** *interface-pool-name* command to check the status of the logging function during IP allocation of the DHCP server.

Prerequisites

The DHCP server function of the interface address pool has been enabled on interfaces using the **dhcp select interface** command.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

- With this logging function enabled, if a large number of DHCP clients request IP addresses from the DHCP server, the server frequently records logs. The server performance may therefore be affected.
- IP address allocation logs are recorded in the AM module. To view log information, the information center must be enabled. In addition, default settings for log output vary depending on various factors including the log level and output direction. For details, see Information Center Configuration.

  For example, the level of logs indicating that an IP address is successfully allocated, an IP address is successfully renewed, and an IP address is successfully released is informational, and these logs are not recorded in the log buffer by default. You can run the **info-center source AM channel 4 log level informational** command to change the level of the logs to be recorded in the log buffer. You can then run the **display logbuffer** command to check the preceding logs.

Example

Enable the logging function during IP address allocation of the DHCP server on the interface VLANIF100.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface vlanif 100
[Huawei-Vlanif100] ip address 192.168.1.1 24
[Huawei-Vlanif100] dhcp select interface
[Huawei-Vlanif100] dhcp server logging
```

Related Topics

8.3.71 display ip pool

8.3.45 dhcp server mask

Function

The **dhcp server mask** command sets the subnet mask of IP addresses that a DHCP server pre-allocates to DHCP clients.

The **undo dhcp server mask** command deletes the configured subnet mask.

By default, the subnet mask of IP addresses that a DHCP server pre-allocates to DHCP clients is not configured.

Format

dhcp server mask { *mask* | *mask-length* }

undo dhcp server mask

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
mask	Specifies a subnet mask.	The value is in decimal dotted notation.
mask-length	Specifies the length of the subnet.	The value is an integer ranging from 0 to 32.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling the DHCP server function on an interface, you can configure the range and subnet mask of IP addresses that a DHCP server pre-allocates to DHCP clients. Run the **dhcp server ip-range** command to configure the IP address range and run the **dhcp server mask** command to configure the subnet mask of the IP addresses.

Prerequisites

The DHCP server function of the interface address pool has been enabled on interfaces using the **dhcp select interface** command.

Example

Set the subnet mask of IP addresses that a DHCP server on a GE1/0/0 pre-allocates to DHCP clients to 255.255.255.0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server mask 255.255.255.0
```

8.3.46 dhcp server nbns-list

Function

The **dhcp server nbns-list** command configures Network Basic Input Output System (NetBIOS) server addresses for an interface address pool.

The **undo dhcp server nbns-list** command deletes the NetBIOS server address from an interface address pool.

By default, no NetBIOS server address is configured for an interface address pool.

Copyright © Huawei Technologies Co., Ltd.

Format

dhcp server nbns-list *ip-address* &<1-8>

undo dhcp server nbns-list { *ip-address* | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies the NetBIOS server address.	The value is in dotted decimal notation.
all	Deletes all NetBIOS server addresses.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. Before hosts communicate with each other, a NetBIOS server needs to resolve the accessed NetBIOS hostname to an IP address. To enable hosts to communicate with each other, run the **dhcp server nbns-list** command to configure NetBIOS server addresses for an interface address pool. When assigning IP addresses to clients, a DHCP server also assigns the configured NetBIOS server addresses to clients. To configure NetBIOS server addresses for a global address pool, run the **nbns-list** command.

Prerequisites

- The address of an interface address pool has been configured using the **ip address** command.
- The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Precautions

Each interface can be configured with a maximum of eight NetBIOS server addresses. The first assigned address functions as the primary address, and other addresses function as secondary addresses.

Example

Specify a NetBIOS server at 192.168.1.99 for domain name resolution when IP addresses in the interface address pool on GE1/0/0 are assigned to clients.

```
<Huawei> system-view
[Huawei] dhcp enable
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.10.10.10 24
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server nbns-list 192.168.1.99
```

Related Topics

8.3.26 dhcp select interface

8.3.47 dhcp server netbios-type

8.3.90 nbns-list

8.3.91 netbios-type

8.3.47 dhcp server netbios-type

Function

The **dhcp server netbios-type** command specifies the NetBIOS node type for a DHCP client connecting to an interface.

The **undo dhcp server netbios-type** command deletes the specified NetBIOS node type of a DHCP client connecting to an interface.

By default, no NetBIOS node type is specified for a DHCP client connecting to an interface.

Format

dhcp server netbios-type { **b-node** | **h-node** | **m-node** | **p-node** }

undo dhcp server netbios-type

Parameters

Parameter	Description	Value
b-node	Indicates a node in broadcast mode. A b-node obtains the mapping in broadcast mode.	-
h-node	Indicates a node in hybrid mode. An h-node is a b-type node enabled with the end-to-end communication mechanism.	-
m-node	Indicates a node in mixed mode. An m-node is a p-type node with some broadcast features.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
p-node	Indicates a node in peer-to-peer mode. This node obtains mappings by communicating with the NetBIOS server.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. When DHCP clients use NetBIOS on the WAN to communicate, their host names and IP addresses need to be mapped. You can run the **dhcp server netbios-type** command to configure the NetBIOS node type for an interface address pool. When assigning an IP address to the client, the DHCP server also sends the specified NetBIOS node type to the client.

Prerequisites

- The address of an interface address pool has been configured using the **ip address** command.
- The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Precautions

To specify the NetBIOS node type for a client in the global address pool, run the **netbios-type** command.

Example

Set the NetBIOS node type for a client in the address pool on GE1/0/0 to **p-node**.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.10.10.10 24
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server netbios-type p-node
```

Related Topics

8.3.26 dhcp select interface

8.3.46 dhcp server nbns-list

8.3.90 nbns-list

Copyright © Huawei Technologies Co., Ltd.

8.3.91 netbios-type

8.3.48 dhcp server next-server

Function

The **dhcp server next-server** command specifies a server IP address for DHCP clients.

The **undo dhcp server next-server** command cancels the configuration.

By default, no server IP address is specified by the DHCP Server for DHCP clients.

Format

dhcp server next-server *ip-address*

undo dhcp server next-server

Parameters

Parameter	Description	Value
ip-address	Specifies a server IP address.	The value is in dotted decimal notation.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp server next-server** command is used on DHCP servers. When assigning a DHCP client an IP address, a DHCP server can also assign the DHCP client an IP address of the server that provides network services for the client. For example, some clients like IP phones still need other configuration parameters after automatically obtaining IP addresses. You can run the **dhcp server next-server** command to specify the server address used after a client obtains an IP address. The client then requests the configuration parameters from the specified server after obtaining an IP address.

If users use addresses in the interface address pool, run the **dhcp server next-server** command to specify the DHCP server IP address. If users use addresses in the global address pool, run the **next-server** command to specify the DHCP server IP address.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

- The address of an interface address pool has been configured using the **ip address** command.
- The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Precautions

- The **dhcp server next-server** command takes effect for only users that use addresses in the interface address pool.
- If you run the **dhcp server next-server** command multiple times, only the latest configuration takes effect.

Example

Specify the server IP address 192.168.1.2 in the interface address pool on VLANIF100 used to provide services for terminal users.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface vlanif 100
[Huawei-Vlanif100] ip address 10.1.1.2 24
[Huawei-Vlanif100] dhcp select interface
[Huawei-Vlanif100] dhcp server next-server 192.168.1.2
```

Related Topics

8.3.93 next-server

8.3.49 dhcp server option

Function

The **dhcp server option** command sets user-defined option for an interface address pool.

The **undo dhcp server option** command deletes user-defined option from an interface address pool.

By default, no user-defined option is configured in an interface address pool.

Format

dhcp server option *code* [**sub-option** *sub-code*] { **ascii** *ascii-string* | **hex** *hex-string* | **cipher** *cipher-string* | **ip-address** *ip-address* &<1-8> }

undo dhcp server option [*code* [**sub-option** *sub-code*]]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
code	Specifies the code for a user-defined option.	The value is an integer that ranges from 1 to 254, except values 1, 3, 6, 15, 44, 46, 50, 51, 52, 53, 54, 55, 57, 58, 59, 61, 82, 120, 121 and 184. **NOTE** • The format of option82, Option121 and Option184 are different from the other codes of a customized option. • There are well-known options and customized options. For details about well-known options, see RFC 2132.
sub-option *sub-code*	Specifies the code of a user-defined sub-option.	The value is an integer that ranges from 1 to 254. For details about well-known options, see RFC 2132.
ascii *ascii-string*	Specifies the user-defined option code as an ASCII character string.	The value is a string of 1 to 255 characters when **sub-option** is not specified, or a string of 1 to 253 characters when **sub-option** is specified.
hex *hex-string*	Specifies the user-defined option code as a hexadecimal string.	The value is a hexadecimal string with an even number of digits, for example, hh or hhhh. If **sub-option** is not specified, the even number is in the range of 2 to 254. If **sub-option** is specified, the even number is in the range of 2 to 252. The value can be a combination of digits (0-9) and letters (A-F and a-f).

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cipher *cipher-string*	Specifies the user-defined option code as a ciphertext character string.	The value is a string, you can enter a character string in explicit text or cipher text. • The character string in explicit text is a string of 1 to 64 characters. • The character string in cipher text is a string of 48 to 108 characters. No matter whether the character string is entered in explicit or cipher text, the character string is displayed in cipher text in the configuration file and in explicit text in packets.
ip-address *ip-address*	Specifies the user-defined option code as an IP address.	The value is in dotted decimal notation.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. The Option field in a DHCP packet carries control information and parameters, including basic information such as the DNS service, NetBIOS service, and IP address lease. If a DHCP server is configured with option, when a DHCP client applies for an IP address from an interface address pool, the client can obtain configurations in the Option field of the DHCP response packet from the DHCP server without having to configure the DNS service, NetBIOS service, or IP address lease separately.

Prerequisites

- The address of an interface address pool has been configured using the **ip address** command.

 Copyright © Huawei Technologies Co., Ltd.

- The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Precautions

- When the password is contained in option, the **ascii** or **hex** type is insecure. Set the option type to **cipher**. A secure password should contain at least two types of the following: lowercase letters, uppercase letters, number, and special characters. In addition, the password must consist of six or more than six characters.
- The **dhcp server option** command configures basic functions, such as the NetBIOS service and IP address lease. The system also provides commands to configure these functions separately. These commands take precedence over the **dhcp server option** command.
- To set user-defined option for a global address pool, run the **option** command.

Example

Set Option64 to 0x11 (a hexadecimal number) for the interface address pool on GE1/0/0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.10.10.10 24
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server option 64 hex 11
```

Related Topics

8.3.26 dhcp select interface

8.3.94 option

8.3.50 dhcp server option121

Function

The **dhcp server option121** command configures a classless static route allocated by a DHCP server to a client.

The **undo dhcp server option121** command deletes a classless static route allocated by a DHCP server to a client.

By default, the classless static route allocated to a client is not configured.

Format

dhcp server option121 ip-address { *ip-address mask-length gateway-address* } &<1-8>

undo dhcp server option121 [**ip-address** *ip-address mask-length gateway-address*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip-address	Specifies the destination IP address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer that ranges from 0 to 32.
gateway-address	Specifies the gateway address of a route.	The value is in dotted decimal notation.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp server option121 ip-address** command applies to only the DHCP server. The **dhcp server option121 ip-address** command configures Option 121 that defines a classless static route allocated to a client from an interface address pool.

mask-length and *gateway-address* specify a classless static route. The **dhcp server option121 ip-address** command configures a maximum of eight classless static routes.

Precautions

- To configure multiple classless static routes, run the **dhcp server option121 ip-address** command repeatedly.
- The **undo dhcp server option121** command will delete all classless static routes. To delete one classless static route, run the **undo dhcp server option121 ip-address** *ip-address mask-length gateway-address* command.

Example

Configure a classless static route allocated by a DHCP server to a client in the interface address pool on VLANIF100.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface vlanif 100
[Huawei-Vlanif100] ip address 10.1.1.2 24
[Huawei-Vlanif100] dhcp select interface
[Huawei-Vlanif100] dhcp server option121 ip-address 10.10.10.10 24 192.168.11.11
```

Related Topics

8.3.83 ip pool (system view)

Copyright © Huawei Technologies Co., Ltd.

8.3.49 dhcp server option

8.3.51 dhcp server option184

Function

The **dhcp server option184** command configures Option 184 allocated by a DHCP server to a client.

The **undo dhcp server option184** command deletes Option 184 allocated by a DHCP server to a client.

By default, Option 184 allocated by a DHCP server to a client is not configured.

Format

dhcp server option184 { **as-ip** *ip-address* | **fail-over** *ip-address dialer-string* | **ncp-ip** *ip-address* | **voice-vlan** *vlan-id* }

undo dhcp server option184 [**as-ip** | **fail-over** | **ncp-ip** | **voice-vlan**]

NOTE

AR109, AR109W, AR109GW-L, AR129CGVW-L do not support **voice-vlan** *vlan-id* parameter.

Parameters

Parameter	Description	Value
ncp-ip *ip-address*	Specifies the IP address of the network call processor (NCP).	The value is in dotted decimal notation.
as-ip *ip-address*	Specifies the IP address of the backup NCP.	The value is in dotted decimal notation.
fail-over *ip-address*	Specifies the IP address in the failover route.	The value is in dotted decimal notation.
dialer-string	Specifies the dialer string.	The value is a string of 1 to 64 characters.
voice-vlan *vlan-id*	Specifies the ID of a voice VLAN.	The value is an integer that ranges from 1 to 4094.

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The **dhcp server option184** command applies to only the DHCP server and configures Option 184 allocated by a DHCP server to a client in an interface address pool.

Example

Configure Option 184 allocated by a DHCP server to a client in the interface address pool on VLANIF100.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface vlanif 100
[Huawei-Vlanif100] ip address 10.1.1.2 24
[Huawei-Vlanif100] dhcp select interface
[Huawei-Vlanif100] dhcp server option184 as-ip 10.10.10.10
```

Related Topics

8.3.83 ip pool (system view)

8.3.49 dhcp server option

8.3.52 dhcp server ping

Function

The **dhcp server ping** command sets the maximum number of ping packets to be sent and the maximum response time of a ping packet.

The **undo dhcp server ping** command restores the default setting.

By default, the DHCP server sends 2 ping packets and the maximum response time is 500 ms.

Format

dhcp server ping { **packet** *number* | **timeout** *milliseconds* } *

undo dhcp server ping { **packet** | **timeout** }

Parameters

Parameter	Description	Value
packet *number*	Specifies the maximum number of ping packets to be sent.	The value is an integer ranging from 0 to 10. The value 0 indicates that no ping operation is performed.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
timeout *milliseconds*	Specifies the maximum response time of a ping packet.	The value is an integer that ranges from 0 to 10000, in milliseconds. The value 0 indicates that no ping operation is performed.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. Repetitive IP address assignment will cause IP address conflicts. To solve this problem, before assigning an IP address to a client, the DHCP server needs to send ping packets using the **dhcp server ping** command to check whether the IP address is in use. Address detection checks whether the DHCP server receives any response within a certain period of time. If there is no response within a certain period of time, the DHCP server continues to send ping packets to this address until the number of ping packets reaches the maximum value. If there is still no response, it indicates that the IP address is not in use. This ensures that the IP address assigned to the client is unique.

Prerequisites

DHCP has been enabled using the **dhcp enable** command.

Example

Set the maximum number of ping packets to 3 and the maximum response time to 400 ms.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp server ping packet 3
[Huawei] dhcp server ping timeout 400
```

Related Topics

8.3.18 dhcp enable

8.3.53 dhcp server sip-server

Copyright © Huawei Technologies Co., Ltd.

Function

The **dhcp server sip-server** command configures the SIP server IP address assigned to a DHCP client on an interface address pool.

The **undo dhcp server sip-server** command deletes the configured SIP server IP address assigned to a DHCP client on an interface address pool.

By default, the SIP server IP address assigned to a DHCP client on an interface address pool is not configured.

Format

dhcp server sip-server { **ip-address** *ip-address* &<1-2> | **list** *domain-name* &<1-2> }

undo dhcp server sip-server

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies an IP address for the SIP server.	The value is in dotted decimal notation.
list *domain-name*	Specifies the domain name of the SIP server.	The value is a string of 1 to 63 characters.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to the DHCP server. To enable DHCP clients to normally access the Internet, the DHCP server needs to specify the SIP server IP address in the interface address pool when assigning IP addresses to the clients.

Precautions

- A maximum of two SIP server addresses can be configured in each address pool. The first assigned address functions as the primary address, and the other address functions as a secondary address.
- Before specifying the IP address or name for a SIP server, ensure that the SIP server exists.
- If you run this command repeatedly, the latest configuration overrides the previous ones.

 Copyright © Huawei Technologies Co., Ltd.

Example

Specify 10.1.1.1 as the IP address of the SIP server when addresses in the interface VLANIF100 address pool are assigned to clients.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server sip-server ip-address 10.1.1.1
```

8.3.54 dhcp server sname

Function

The **dhcp server sname** command configures the name of the server where the DHCP client obtains the startup configuration file.

The **undo dhcp server sname** command deletes the configured name of the server where the DHCP client obtains the startup configuration file.

By default, the name of the server where the DHCP client obtains the startup configuration file is not configured.

Format

dhcp server sname *sname*

undo dhcp server sname

Parameters

Parameter	Description	Value
sname	Specifies the name of the server where the DHCP client obtains the startup configuration file.	The value is a string of 1 to 63 case-sensitive characters without spaces.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Besides assigning IP addresses, a DHCP server can also provide the required network configuration parameters, such as the startup configuration file name for

 Copyright © Huawei Technologies Co., Ltd.

the DHCP clients. After the name of the server where the DHCP client obtains the startup configuration file is configured using the **dhcp server sname** command, the DHCP client obtains the startup configuration file from this server.

Prerequisites

1. The DHCP function has been enabled using the **8.3.18 dhcp enable** command in the system view.
2. The DHCP server has been enabled on the interface using the **8.3.26 dhcp select interface** command.
3. The startup configuration file name has been configured for the DHCP client using the **8.3.29 dhcp server bootfile**.

Follow-up Procedures

Ensure that the route between the DHCP client and the file server where the DHCP client obtains the startup configuration file is reachable.

Example

Configure the name of the server where the DHCP client obtains the startup configuration file as **Huawei** in the interface address pool on GE1/0/0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.1.1.1 255.255.255.0
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server bootfile start.ini
[Huawei-GigabitEthernet1/0/0] dhcp server sname Huawei
```

Related Topics

8.3.18 dhcp enable

8.3.26 dhcp select interface

8.3.29 dhcp server bootfile

8.3.55 dhcp server static-bind

Function

The **dhcp server static-bind** command binds an IP address in an interface address pool to a MAC address.

The **undo dhcp server static-bind** command unbinds the IP address in an interface address pool from a MAC address.

By default, an IP address in an interface address pool is not bound to any MAC address.

Format

dhcp server static-bind ip-address *ip-address* **mac-address** *mac-address* [**description** *description*]

undo dhcp server static-bind [**ip-address** *ip-address* | **mac-address** *mac-address*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the IP address to be bound. The IP address must be valid in an interface address pool.	The value is in dotted decimal notation.
mac-address *mac-address*	Specifies the user MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
description *description*	Specifies the user description.	The value is a string of 1 to 256 case-sensitive characters. It can contain spaces.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp server static-bind** command applies to DHCP servers. When planning a network, you need to allocate fixed IP addresses to some important hosts to ensure reliability. In this case, you can bind IP addresses in the address pool to the MAC addresses of these hosts. After the preceding configuration is complete, if the host of the MAC address to which the IP address is bound request an IP address from the DHCP server, the DHCP server finds the bound IP address based on the host's MAC address and allocates this IP address to the host, ensuring that the IP address obtained by the host is fixed.

You can run the **dhcp server static-bind** command to bind an IP address in an interface address pool to a MAC address.

You can run the **static-bind** command to bind an IP address in a global address pool to a MAC address.

Prerequisites

- The address of an interface address pool has been configured using the **ip address** command.
- Enable the DHCP server function based on the interface address pool on the interface using the **dhcp select interface** command.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

- Ensure that the bound IP address is not configured as the IP address that cannot be allocated using the **8.3.36 dhcp server excluded-ip-address** command and is not allocated by the DHCP server.
- You can run the **display ip pool** command to view the used IP addresses in the current address pool and select an available IP address to be bound to the MAC address. To bind used IP addresses to MAC addresses, run the **reset ip pool** command to reclaim used IP addresses first. IP addresses that are used can also be statically bound to MAC addresses or unbound from MAC addresses. When an IP address is statically bound to a MAC address, ensure that the MAC address to be bound is the same as the MAC address of the user who actually uses the IP address.
- The DHCP server preferentially allocates the IP address that has been statically bound to the client's MAC address.
- After an IP address is bound to a MAC address, the IP address does not expire; the binding between the IP and MAC addresses cannot be deleted when the IP address is in use. After an IP address is bound to a MAC address, the IP address does not expire. After an automatically allocated IP address is statically bound to a MAC address, the lease time of the IP address becomes unlimited. After the static binding between the IP address and the MAC address is deleted, the lease time of the IP address becomes the same as that configured in the address pool.

Example

Configure a DHCP server to assign a fixed IP address 10.10.10.20 in the interface address pool on gigabitethernet 1/0/0 to a host with the MAC address 2020-e2f3-2a3b.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.10.10.10 24
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server static-bind ip-address 10.10.10.20 mac-address 2020-e2f3-2a3b
```

8.3.56 dhcp server trust option82

Function

The **dhcp server trust option82** command enables Option 82 on the DHCP server.

The **undo dhcp server trust option82** command disables Option 82 on the DHCP server.

By default, the DHCP server trusts Option 82.

Format

dhcp server trust option82

undo dhcp server trust option82

Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on the DHCP server to enable the Option 82 function. After receiving a DHCP packet that carries the Option 82 field but the giaddr is 0, the DHCP server processes the packet by default. Using the **undo dhcp server trust option82** command, the DHCP server discards the packet.

Prerequisites

DHCP has been enabled globally by using the **dhcp enable** command.

Example

Enable Option 82 of the DHCP server.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp server trust option82
```

8.3.57 dhcp set ttl

Function

The **dhcp set ttl** command sets the TTL value for DHCP Discover messages after they are forwarded by the DHCP relay agent at Layer 3.

The **undo dhcp set ttl** command restores the default setting.

By default, the TTL value of DHCP Discovery messages decreases by 1 after they are forwarded by the DHCP relay agent at Layer 3.

Format

dhcp set ttl { **unvaried** | *ttl-value* }

undo dhcp set ttl

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
unvaried	Indicates that the TTL value of DHCP Discovery messages remains unchanged after the messages are forwarded by the DHCP relay agent at Layer 3. That is, the device does not reduce the TTL value by 1.	-
ttl-value	Specifies a fixed TTL value for DHCP Discovery messages after they are forwarded by the DHCP relay agent at Layer 3.	The value is an integer that ranges from 1 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp set ttl** command is used on DHCP relay agents. When a DHCP relay agent forwards DHCP Discovery messages at Layer 3, it reduces the TTL value of the messages by 1 by default. Assume that the TTL value of a DHCP Discovery message received by the DHCP relay agent is 1. If the DHCP relay agent reduces the TTL value by 1, the TTL value changes to 0. The next-hop routing device will discard the message as its TTL value is 0. As a result, the DHCP server cannot receive the DHCP Discovery message forwarded by the DHCP relay agent. To ensure that the DHCP server can receive the DHCP Discovery message sent from the client, run the **dhcp set ttl** command to set the TTL value of the DHCP Discovery message to a non-zero value after the message is forwarded at Layer 3.

NOTE

If the DHCP relay agent connects to a special client whose TTL value of DHCP Discovery messages is 1, and if there are routing devices between the DHCP relay agent and DHCP server, run the **dhcp set ttl** *ttl-value* command to specify a fixed TTL value (16 is recommended) for DHCP Discovery messages after they are forwarded by the DHCP relay agent at Layer 3.

Prerequisites

The DHCP function has been enabled globally using the **dhcp enable** command.

Example

Set the TTL value of DHCP Discovery messages to 16 after the messages are forwarded by the DHCP relay agent at Layer 3.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp set ttl 16
```

8.3.58 dhcp speed-limit auto

Function

The **dhcp speed-limit auto** command enables dynamic rate limiting on DHCP packets.

The **undo dhcp speed-limit auto** command disables dynamic rate limiting on DHCP packets.

By default, dynamic rate limiting is disabled on DHCP packets.

Format

dhcp speed-limit auto

undo dhcp speed-limit auto

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure security or facilitate management, users may require that the DHCP packet processing rate should be limited. If the rate is not limited, CPU and memory resources can be used up due to malicious attacks.

Table 8-21 and **Table 8-22** list the mapping between the DHCP packet rate and CPU/memory usage after dynamic rate limiting on DHCP packets is enabled.

Table 8-21 DHCP packet rate and CPU usage

CPU Usage (%)	DHCP Packet Rate (packets/second)
(70–85)	100
[85–100)	50
100	10

Copyright © Huawei Technologies Co., Ltd.

Table 8-22 DHCP packet rate and memory usage

Memory Usage (%)	DHCP Packet Rate (packets/second)
(65–75)	100
[75–85)	50
[85–100)	10

Prerequisites

DHCP has been enabled globally by using the **dhcp enable** command.

Precautions

- When the CPU usage is higher than 70% or the memory usage is higher than 65%, the DHCP packet processing rate is limited.
- The DHCP packet processing rate is the same as the smaller rate among the rates corresponding to the CPU or memory usage. For example, when the CPU usage is 80% and the memory usage is 80%, the DHCP packet rate is 50.

Example

Enable dynamic rate limiting on DHCP packets.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp speed-limit auto
```

8.3.59 dhcp-server

Function

The **dhcp-server** command adds DHCP servers to a DHCP server group.

The **undo dhcp-server** command deletes DHCP servers from a DHCP server group.

By default, no DHCP server is configured in a DHCP server group.

Format

dhcp-server *ip-address* [*ip-address-index*]

undo dhcp-server { *ip-address* | *ip-address-index* }

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a DHCP server.	The value is in dotted decimal notation.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ip-address-index	When you specify the IP address for a DHCP server, you can specify *ip-address-index* for the IP address. If you do not specify the server index, the system assigns an idle index to the server.	The value is an integer that ranges from 0 to 7.

Views

DHCP server group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp-server** command applies to DHCP relay agents. To ensure that the DHCP relay agent can forward messages to multiple DHCP servers, configure multiple DHCP servers in a DHCP server group.

Precautions

- Each DHCP server group can be configured with a maximum of eight DHCP servers. You can delete a DHCP server by specifying *ip-address-index*.
- If a VPN instance is bound to an interface of the router, the DHCP server group must be bound to this VPN instance.

Example

Add the DHCP server at 10.10.78.56 to a DHCP server group **dhcp-srv1**.

```
<Huawei> system-view
[Huawei] dhcp server group dhcp-srv1
[Huawei-dhcp-server-group-dhcp-srv1] dhcp-server 10.10.78.56
```

Related Topics

8.3.40 dhcp server group
8.3.68 display dhcp server group
8.3.23 dhcp relay server-select

8.3.60 display dhcp client

Function

The **display dhcp client** command displays DHCP/BOOTP client lease information.

Copyright © Huawei Technologies Co., Ltd.

Format

display dhcp client [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays DHCP/BOOTP client lease information on a specified interface: • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When a device functions as the DHCP/BOOTP client, this command displays DHCP/BOOTP client lease information.

Example

Display DHCP client lease information.

```
<Huawei> display dhcp client
DHCP client lease information on interface GigabitEthernet0/0/1 :
 Current machine state         : Bound
 Internet address assigned via : DHCP
 Physical address              : 0819-a6cd-a896
 IP address                    : 192.168.1.254
 Subnet mask                   : 255.255.255.0
 Gateway ip address            : 192.168.1.2
 DHCP server                   : 192.168.1.2
 Lease obtained at             : 2013-06-26 07:40:22
 Lease expires at              : 2013-06-27 07:40:22
 Lease renews at               : 2013-06-26 19:40:22
 Lease rebinds at              : 2013-06-27 04:40:22
```

 Copyright © Huawei Technologies Co., Ltd.

Table 8-23 Description of the **display dhcp client** command output

Item	Description
DHCP client lease information on interface *if1*	DHCP client lease information on the interface *if1*.
Current machine state	Current device status.
Internet address assigned via	IP address obtained using DHCP or BOOTP.
Physical address	Device MAC address.
IP address	Device IP address.
Subnet mask	Mask of the device IP address.
Gateway ip address	Gateway address of the DHCP or BOOTP server.
DHCP server	DHCP server address (no value for a BOOTP client).
Lease obtained at	Time the lease is obtained.
Lease expires at	Time the lease expires (no value for a BOOTP client).
Lease renews at	Time the lease needs to be renewed (no value for a BOOTP client). The lease of an IP address needs to be renewed when half of the lease expires.
Lease rebinds at	Time the lease is renewed (no value for a BOOTP client). The lease of an IP address is renewed when 87.5% of the lease expires.

8.3.61 display dhcp client statistics

Function

The **display dhcp client statistics** command displays message statistics on a DHCP/BOOTP client.

Format

display dhcp client statistics [**interface** *interface-type interface-number*]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays message statistics on a specified interface: • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the device functions as the DHCP client, the **display dhcp client statistics** command displays message statistics.

Example

Display message statistics on a DHCP/BOOTP client.

```
<Huawei> display dhcp client statistics
DHCP message statistics on interface Ethernet2/0/0 :
Input: total 0 packets
  Bootp reply            :         0
  Offer                  :         0
  Ack                    :         0
  Nak                    :         0
Output: total 0 packets
  Bootp request          :         0
  Discover               :         0
  Request                :         0
    Request of init-reboot:         0
    Request of selecting  :         0
    Request of renewing   :         0
    Request of rebinding  :         0
  Decline                :         0
  Release                :         0
```

Table 8-24 Description of the **display dhcp client statistics** command output

Item	Description
Input	Total number of DHCP messages received by the client.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Bootp reply	Number of BOOTP replies received by the client from the server.
Offer	Number of Offer messages received by the client from the server.
Ack	Number of ACK messages received by the client from the server.
Nak	Number of NAK messages received by the client from the server.
Output	Total number of messages forwarded by the client.
Bootp request	Number of BOOTP requests received by the server from the client.
Discover	Number of Discover messages received by the server from the client.
Request	Number of Request messages received by the server from the client.
Request of init-reboot	Number of Request of init-reboot messages received by the server from the client.
Request of selecting	Number of Request of selecting messages received by the server from the client.
Request of renewing	Number of Request of renewing messages received by the server from the client.
Request of rebinding	Number of Request of rebinding messages received by the server from the client.
Decline	Number of Decline messages received by the server from the client.
Release	Number of Release messages received by the server from the client.

8.3.62 display dhcp server configuration

Function

The **display dhcp server configuration** command displays configurations about a DHCP server.

 Copyright © Huawei Technologies Co., Ltd.

Format

display dhcp server configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the Router functions as a DHCP server, you can run the **display dhcp server configuration** command to display configurations about the DHCP server.

Example

Display configurations about a DHCP server.

```
<Huawei> display dhcp server configuration
  DHCP server global running information :
  DHCP server bootp                : Disable (default)
  DHCP server bootp automatic      : Disable (default)
  DHCP server ping packet          : 2       (default)
  DHCP server ping timeout         : 500     (default)
  DHCP server trust option82       : Enable  (default)
  DHCP server force response       : Disable (default)

  DHCP server running information for interface Vlanif10 :
  DHCP server mode                 : Interface

  DHCP server running information for interface
Vlanif20 :
  DHCP server mode                 : Global
```

Table 8-25 Description of the **display dhcp server configuration** command output

Item	Description
DHCP server global running information	Global configurations about the DHCP server.
DHCP server bootp	Whether the DHCP server is enabled to respond to BOOTP requests. To configure this item, run the **8.3.30 dhcp server bootp** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
DHCP server bootp automatic	Whether the DHCP server is enabled to dynamically allocate IP addresses to BOOTP clients. To configure this item, run the **8.3.31 dhcp server bootp automatic** command.
DHCP server ping packet	Maximum number of ping packets sent by the DHCP server. To configure this item, run the **8.3.52 dhcp server ping** command.
DHCP server ping timeout	Maximum response time of a ping packet sent by the DHCP server. To configure this item, run the **8.3.52 dhcp server ping** command.
DHCP server trust option82	Whether the DHCP server is enabled to trust the Option82 field. To configure this item, run the **8.3.56 dhcp server trust option82** command.
DHCP server force response	Whether the DHCP server is enabled to reply with DHCP NAK messages. To configure this item, run the **8.3.39 dhcp server force response** command.
DHCP server running information for interface *ifn*	Configurations about the DHCP server on an interface.
DHCP server mode	DHCP server mode. The value can be: • Interface: DHCP server based on an interface address pool. To configure this item, run the **8.3.26 dhcp select interface** command. • Global: DHCP server based on the global address pool. To configure this item, run the **8.3.25 dhcp select global** command.

8.3.63 display dhcp configuration

Function

The **display dhcp configuration** command displays configuration information about the DHCP public module.

Format

display dhcp configuration

Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command is used to query configuration information about the DHCP public module.

Example

Display configuration information about the DHCP public module.

```
<Huawei> display dhcp configuration
  DHCP global running information :
  DHCP                                : Enable
  DHCP speed limit                        : Disable  (default)
```

Table 8-26 Description of the **display dhcp configuration** command output

Item	Description
DHCP global running information	Configuration information about the DHCP public module in the system view.
DHCP	Indicates whether DHCP is enabled. The value can be: • Enable: DHCP is enabled. • Disable (default): DHCP is disabled. By default, DHCP is disabled. You can configure this parameter using the **8.3.18 dhcp enable** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
DHCP speed limit	Indicates whether dynamic DHCP message rate limiting is enabled. The value can be: • Enable: Dynamic DHCP message rate limiting is enabled. • Disable (default): Dynamic DHCP message rate limiting is disabled. By default, dynamic DHCP message rate limiting is disabled. You can configure this parameter using the **8.3.58 dhcp speed-limit auto** command.

8.3.64 display dhcp option template

Function

The **display dhcp option template** command displays the configuration of a DHCP Option template.

Format

display dhcp option template [**name** *template-name*]

Parameters

Parameter	Description	Value
name *template-name*	Displays the configuration of a specified DHCP Option template.	The template must be an existing DHCP Option template.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring a DHCP Option template, you can run the **display dhcp option template** command to view the configuration of the DHCP Option template,

Copyright © Huawei Technologies Co., Ltd.

including the template name, number, IP address of a server configured for the client after the client automatically obtains the IP address, domain name, and values of customized options.

Example

Display the configuration of the DHCP Option template named **test**.

```
<Huawei> display dhcp option template name test
 ------------------------------------------------------------------------------
 Template-Name  : test
 Template-No    : 1
 Next-server    : 192.168.1.5
 Domain-name    : huawei.com
 DNS-server0    : 192.168.2.7
 DNS-server1    : 192.168.2.8
 NBNS-server0   : 192.168.1.7
 NBNS-server1   : 192.168.1.8
 Netbios-type   : b-node
 Gateway-0      : 192.168.1.10
```

Display the configurations of all DHCP Option templates.

```
<Huawei> display dhcp option template
 ------------------------------------------------------------------------------
 Template-Name  : template1
 Template-No    : 0
 Next-server    : 10.1.1.4
 Domain-name    : -
 DNS-server0    : -
 NBNS-server0   : -
 Netbios-type   : -
 Gateway-0      : -

 ------------------------------------------------------------------------------
 Template-Name  : template2
 Template-No    : 1
 Next-server    : 192.168.1.5
 Domain-name    : huawei.com
 Option-code    : 64
   Option-subcode : 3
     Option-type  : hex
     Option-value : 11
 DNS-server0    : 192.168.2.7
 DNS-server1    : 192.168.2.8
 NBNS-server0   : 192.168.2.7
 NBNS-server1   : 192.168.2.8
 Netbios-type   : b-node
 Gateway-0      : 192.168.1.10
```

Table 8-27 Description of the **display dhcp option template** command output

Item	Description
Template-Name	Name of the DHCP Option template. To specify the parameter, run the **8.3.20 dhcp option template** command.
Template-No	Index value of the DHCP Option template.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Next-server	IP address of a server configured for the client after the client automatically obtains the IP address. To specify the parameter, run the **8.3.93 next-server** command in the DHCP Option template view.
Domain-name	Name of a domain. To specify the parameter, run the **8.3.76 domain-name** command in the DHCP Option template view.
Option-code	Code for a customized option. To specify the parameter, run the **8.3.94 option** command in the DHCP Option template view.
Option-subcode	Code for a customized sub-option. To specify the parameter, run the **8.3.94 option** command in the DHCP Option template view.
Option-type	Character string type for a customized option. To specify the parameter, run the **8.3.94 option** command in the DHCP Option template view.
Option-value	Character string value for a customized option. To specify the parameter, run the **8.3.94 option** command in the DHCP Option template view.
DNS-server0	Address of the DNS server. Currently, a maximum of eight DNS server addresses can be configured. Values 0 and 1 indicate the first and second DNS server addresses respectively. To specify the parameter, run the **8.3.75 dns-list** command in the DHCP Option template view.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
NBNS-server0	Address of the NetBIOS server. Currently, a maximum of eight NetBIOS server addresses can be configured in a DHCP Option template. Values 0 and 1 indicate the first and second NetBIOS server addresses respectively. To specify the parameter, run the **8.3.90 nbns-list** command in the DHCP Option template view.
Netbios-type	NetBIOS node type. To specify the parameter, run the **8.3.91 netbios-type** command in the DHCP Option template view.
Gateway-0	Gateway address. Currently, a maximum of eight gateway addresses can be configured. The value 0 indicates the first gateway address. To specify the parameter, run the **8.3.80 gateway-list** command in the DHCP Option template view.

Related Topics

8.3.20 dhcp option template

8.3.65 display dhcp relay

Function

The **display dhcp relay** command displays configuration information about a DHCP relay agent.

Format

display dhcp relay { **all** | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
all	Displays configuration information about DHCP relay agents configured on all interfaces.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface *interface-type interface-number*	Displays configuration information about a DHCP relay agent configured on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check configuration information about DHCP relay agents configured on interfaces.

Example

Display configuration information about DHCP relay agents on all interfaces.

```
<Huawei> display dhcp relay all
 DHCP relay agent running information of interface Vlanif5 :
 Server group name      : group1
 Gateway address in use : 10.100.100.1

 DHCP relay agent running information of interface Vlanif100 :
 Server IP address [00] : 10.2.2.3
 Gateway address in use : 10.2.2.2
```

Table 8-28 Description of the **display dhcp relay all** command output

Item	Description
DHCP relay agent running information of interface *if*	DHCP relay agent configuration of the *if* interface.
Server group name	Group name of the DHCP Server. To specify the parameter, run the **8.3.23 dhcp relay server-select** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Server IP address [x]	IP address of a DHCP server in the DHCP server group. The value x is the index of a DHCP server. To specify the parameter, run the **8.3.59 dhcp-server** command.
Gateway address in use	IP address of the DHCP gateway. To specify the parameter, run the **8.3.79 gateway (DHCP server group view)** command.

8.3.66 display dhcp relay statistics

Function

The **display dhcp relay statistics** command displays message statistics on a DHCP relay agent.

Format

display dhcp relay statistics [**server-group** *group-name*]

Parameters

Parameter	Description	Value
server-group *group-name*	Displays message statistics on DHCP relay agents connected to DHCP servers in a specified DHCP server group. If this parameter is not specified, message statistics on DHCP relay agents connected to all DHCP servers are displayed.	The value must be an existing DHCP server group on the device.

Views

All views

Default Level

1: Monitoring level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

Run the **display dhcp relay statistics** command to check whether the client is correctly configured or the network is connected.

- Run the **display dhcp relay statistics server-group** *group-name* command to check message statistics on DHCP relay agents connected to DHCP servers in a specified DHCP server group. The DHCP server group name needs to be specified.
- Run the **display dhcp relay statistics** command to check message statistics on all DHCP relay agents besides DHCP relay agents connected to DHCP servers in the DHCP server group.

Follow-up Procedure

After detecting incorrect message statistics on a DHCP relay agent, run the **reset dhcp relay statistics** [**server-group** *group-name*] command to clear message statistics on the DHCP relay agent.

Example

Display message statistics on a DHCP relay agent.

```
<Huawei> display dhcp relay statistics
  The statistics of DHCP RELAY:
    DHCP packets received from clients        : 0
        DHCP DISCOVER packets received        : 0
        DHCP REQUEST packets received         : 0
        DHCP RELEASE packets received         : 0
        DHCP INFORM packets received          : 0
        DHCP DECLINE packets received         : 0
    DHCP packets sent to clients              : 0
        Unicast packets sent to clients       : 0
        Broadcast packets sent to clients     : 0
    DHCP packets received from servers        : 0
        DHCP OFFER packets received           : 0
        DHCP ACK packets received             : 0
        DHCP NAK packets received             : 0
    DHCP packets sent to servers              : 0
    DHCP Bad packets received                 : 0
```

Table 8-29 Description of the **display dhcp relay statistics** command output

Item	Description
DHCP packets received from clients	DHCP messages received from clients.
DHCP DISCOVER packets received	DHCP Discover messages received from clients.
DHCP REQUEST packets received	DHCP Request messages received from clients.
DHCP RELEASE packets received	DHCP Release messages received from clients.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
DHCP INFORM packets received	DHCP Inform messages received from clients.
DHCP DECLINE packets received	DHCP Decline messages received from clients.
DHCP packets sent to clients	DHCP messages sent to clients.
Unicast packets sent to clients	Unicast packets sent to clients.
Broadcast packets sent to clients	Broadcast packets sent to clients.
DHCP packets received from servers	DHCP messages received from servers.
DHCP OFFER packets received	DHCP Offer messages received from servers.
DHCP ACK packets received	DHCP ACK messages received from servers.
DHCP NAK packets received	DHCP NAK messages received from servers.
DHCP packets sent to servers	DHCP messages sent to servers.
DHCP Bad packets received	DHCP error messages received.

Related Topics

8.3.98 reset dhcp relay statistics
8.3.69 display dhcp server statistics

8.3.67 display dhcp server database

Function

The **display dhcp server database** command displays information about the DHCP database.

Format

display dhcp server database

Parameters

None

Views

All views

Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display dhcp server database** command displays the storage path and file name of DHCP data on a DHCP server. This information helps to check:

- Whether the function that saves DHCP data to the storage device is enabled. If this function is not enabled, run the **dhcp server database** command to enable it.
- Whether the interval at which DHCP data is saved is proper.
- Whether the function that recovers DHCP data from the storage device after the system restarts is enabled.

Precautions

The function that saves DHCP data to storage devices and the function that recovers DHCP data from storage devices can be enabled in any sequence.

Example

Display information about the DHCP database.

```
<Huawei> display dhcp server database
 Status: disable
 Recover from files after reboot: disable
 File saving lease items: flash:/dhcp/lease.txt
 File saving conflict items: flash:/dhcp/conflict.txt
 Save Interval: 300 (seconds)
```

Table 8-30 Description of the **display dhcp server database** command output

Item	Description
Status	Whether to save the data to the storage device: • disable • enable The value is set using the **dhcp server database** command.
Recover from files after reboot	Whether to recover data from the file on the storage device after the system restarts: • disable • enable The value is set using the **dhcp server database** command.
File saving lease items	File name and path of the file for storing address lease information.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
File saving conflict items	File name and path of the file for storing address conflict information.
Save Interval	Interval at which DHCP data is saved, in seconds. The value is set using the **dhcp server database** command.

8.3.68 display dhcp server group

Function

The **display dhcp server group** command displays the configuration of a DHCP server group.

Format

display dhcp server group [*group-name*]

Parameters

Parameter	Description	Value
group-name	Displays the configuration of a specified DHCP server group.	The value must be an existing DHCP server group on the device.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command applies to DHCP relay agents. The **display dhcp server group** command displays information about all the DHCP server groups of a DHCP relay agent and the number of DHCP servers in the DHCP server groups. If *group-name* is specified, the **display dhcp server group** *group-name* command displays DHCP server addresses and the number of DHCP servers in a specified DHCP server group.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

A DHCP server group has been created on a DHCP relay agent using the **dhcp server group** command.

Example

Display the configuration of the DHCP server group **myServers**.

```
<Huawei> display dhcp server group myServers
  Group-name          : myServers
    (0)  Server-IP    : 10.1.1.1
    Gateway           : 10.10.10.1
    VPN instance      : --
```

Table 8-31 Description of the **display dhcp server group** command output

Item	Description
Group-name	Name of a DHCP server group. To specify the parameter, run the **8.3.40 dhcp server group** command.
Gateway	Gateway address of the DHCP server in the DHCP server group. To specify the parameter, run the **8.3.79 gateway (DHCP server group view)** command.
VPN instance	VPN instance to which the DHCP server group belongs. To specify the parameter, run the **8.3.109 vpn-instance (DHCP server group view)** command.

8.3.69 display dhcp server statistics

Function

The **display dhcp server statistics** command displays statistics on a DHCP server.

Format

display dhcp server statistics

Parameters

None

Views

All views

Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the display dhcp server statistics command to check whether the client is correctly configured or the network is connected.

Follow-up Procedure

After detecting incorrect message statistics on a DHCP server, run the **reset dhcp server statistics** command to clear message statistics on the DHCP server.

Example

Display statistics on the DHCP server.

```
<Huawei> display dhcp server statistics
 DHCP Server Statistics:

 Client Request:            6
  Dhcp Discover:            1
  Dhcp Request:             4
  Dhcp Decline:             0
  Dhcp Release:             1
  Dhcp Inform:              0
 Server Reply:              4
  Dhcp Offer:               1
  Dhcp Ack:                 3
  Dhcp Nak:                 0
 Bad Messages:              0
```

Table 8-32 Description of the **display dhcp server statistics** command output

Item	Description
DHCP Server Statistics	Statistics on the DHCP server.
Client Request	Number of DHCP messages sent from the DHCP client to the DHCP server.
Dhcp Discover, Dhcp Request, Dhcp Decline, Dhcp Release, Dhcp Inform	Numbers of different types of DHCP messages sent from the DHCP client to the DHCP server.
Server Reply	Number of DHCP messages sent from the DHCP server to the DHCP client.
Dhcp Offer, Dhcp Ack, Dhcp Nak	Numbers of different types of DHCP messages sent from the DHCP server to the DHCP client.
Bad Messages	Number of unknown messages.

Copyright © Huawei Technologies Co., Ltd.

Related Topics

8.3.99 reset dhcp server statistics

8.3.70 display dhcp statistics

Function

The **display dhcp statistics** command displays DHCP message statistics.

Format

display dhcp statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display dhcp statistics** command displays statistics about sent and received DHCP messages.

Example

Display DHCP message statistics.

```
<Huawei> display dhcp statistics
Input: total 172 packets, discarded 0 packets
  Bootp request          :         0,  Bootp reply          :         0
  Discover               :         0,  Offer                :       172
  Request                :         0,  Ack                  :         0
  Release                :         0,  Nak                  :         0
  Decline                :         0,  Inform               :         0

  Rx buffers full        :      2978,  L2fdb lookup failed    :        38

Output: total 172 packets, discarded 0 packets
```

Table 8-33 Description of the **display dhcp statistics** command output

Item	Description
Bootp request	Number of BOOTP requests sent by the device that functions as the client.
Bootp reply	Number of BOOTP replies received by the client from the server.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Discover	Number of Discover messages received by the server from the client.
Offer	Number of Offer messages received by the client from the server.
Request	Number of BOOTP requests received by the server from the client.
Ack	Number of ACK messages received by the client from the server.
Release	Number of Release messages received by the server from the client.
Nak	Number of NAK messages received by the client from the server.
Decline	Number of Decline messages sent by the client.
Inform	Number of Inform messages sent by the client.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Rx buffers full or L2fdb lookup failed	Information displayed when the DHCP service is abnormal. The displayed information includes: • Rx buffers full: Total number of DHCP packets discarded because the remaining queue length is shorter than the reserved threshold. • L2fdb lookup failed: Total number of DHCP packets discarded because entries fail to be queried. • High cpu occupancy: Total number of DHCP packets discarded because the CPU usage is excessively high. • Port blocked: Total number of DHCP packets discarded because the inbound interface is blocked. • Bad vlan id: Total number of DHCP packets discarded because the VLAN ID is incorrect. • Memory exhausted: Total number of DHCP packets discarded because the memory is exhausted. • L3if protocol down: Total number of DHCP packets discarded because the Layer 3 protocol of the source interface goes Down. • Rate limit: Total number of DHCP packets discarded because rates of the packets exceed the limit. • Bad packet length: Total number of DHCP packets discarded because the packet length is incorrect. • Bad ip header length: Total number of DHCP packets discarded because the IP header length is incorrect. • Bad ip header checksum: Total number of DHCP packets discarded because the checksum of the IP header is incorrect. • Bad udp checksum: Total number of DHCP packets discarded because the checksum of the UDP header is incorrect. • Hops exceeded: Total number of DHCP packets discarded because the number of next hops is incorrect.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• Bad magic cookie: Total number of DHCP packets discarded because the magic-cookie field is incorrect. • Duplicate option: Total number of DHCP packets discarded because the option fields are duplicate. • Bad option length: Total number of DHCP packets discarded because the option field length is incorrect. • End option absent: Total number of DHCP packets discarded because of the incorrect end option. • Dest-port equals source: Total number of DHCP packets discarded because the source interface is also the outbound interface. • Bad chaddr: Total number of DHCP packets discarded because the MAC address of the client is incorrect. • Bad giaddr: Total number of DHCP packets discarded because the relay gateway is incorrect. • Bad request: Total number of DHCP packets discarded because the request packets are incorrect. • Bad reply: Total number of DHCP packets discarded because the response packets are incorrect. • Bad dest udp-port: Total number of DHCP packets discarded because the destination interface is incorrect. • Bad message type: Total number of DHCP packets discarded because of incorrect destination interfaces. • L2fdb lookup failed: Total number of incoming DHCP packets discarded because entries fail to be queried. • Max-user limit: Total number of DHCP packets discarded because the maximum number of users is exceeded. • Add bindtable failed: Total number of DHCP packets discarded because dynamic binding entries are added.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• Client transferred: Total number of DHCP packets discarded due to interface flapping. • Bad original interface: Total number of DHCP packets discarded because dynamic binding entries are added. • Bad client-id: Total number of DHCP packets discarded because the client ID is incorrect. • Bad server-id: Total number of DHCP packets discarded because the server ID is incorrect. • Bad dest-ip: Total number of DHCP packets discarded because the destination IP address is incorrect. • Other error: Total number of DHCP packets discarded due to other reasons.

8.3.71 display ip pool

Function

The **display ip pool** command displays the configurations of an address pool.

Format

display ip pool

display ip pool interface *interface-pool-name* [*start-ip-address* [*end-ip-address*] | **all** | **conflict** | **expired** | **used**]

display ip pool name *ip-pool-name* [*start-ip-address* [*end-ip-address*] | **all** | **conflict** | **expired** | **used** [**user-type** { **dhcp** | **pppoe** | **l2tp** | **ipsec** | **ssl-vpn** | **ppp** }]]

display ip pool vpn-instance *vpn-instance-name*

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface *interface-pool-name*	Displays the configuration of the specified interface address pool. **NOTE** An interface address pool is specified using the type and number of an interface without spaces between them.	The interface address pool must exist on the device.
name *ip-pool-name*	Displays the configuration of the specified global address pool.	The global address pool must exist on the device.
start-ip-address [*end-ip-address*]	Displays the IP addresses within the range specified by the start IP address in the address pool. If *end-ip-address* is set, the end IP address is also specified.	The value is in dotted decimal notation.
all	Displays all IP addresses in the address pool.	-
conflict	Displays the conflicting IP addresses in the address pool. (If an IP address that the DHCP server prepares to allocate to a user exists on the network, the IP address will be added to the conflict list. This problem occurs when a static IP address is configured or an active/standby switchover occurs in a VRRP group if the range of IP addresses in the address pools on the master and backup devices overlap.)	-
expired	Displays the expired and idle IP addresses in the address pool.	-
used [**user-type** { **dhcp** | **pppoe** | **l2tp** | **ipsec** | **ssl-vpn** | **ppp** }]	Display the IP addresses used in the address pool by the specific type of users. • Select **dhcp**, to specify the users who obtain IP addresses by DHCP. • Select **pppoe**, to specify the users who obtain IP addresses by PPPoE dial-up. • Select **l2tp**, to specify the L2TP users. • Select **ipsec**, to specify the IPSec users. • Select **ssl-vpn**, to specify the SSL VPN users. • Select **ppp**, to specify the PPP users.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about the address pool in a specified VPN instance.	The value must be an existing VPN instance on the device.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ip pool** command to view information about a configured address pool and IP addresses in the address pool, including the address pool name, lease, lock status, and status of IP addresses in the address pool.

Example

Display information about conflicting IP addresses in the address pool **huawei**.

```
<Huawei> display ip pool name huawei conflict
  Pool-name        : huawei
  Pool-No          : 1
  Lease            : 1 Days 0 Hours 0 Minutes
  Domain-name      : -
  Option-code      : 60
    Option-subcode : --
    Option-type    : cipher
    Option-value   : %^%#5g)NPN1M,$M;pQ-lT\P>Al6QN4#ldIVVjD69XlCN%^%#
  DNS-server0      : -
  NBNS-server0     : -
  Netbios-type     : -
  Position         : Local
  Status           : Unlocked
  Gateway-0        : -
  Network          : 192.168.0.0
  Mask             : 255.255.255.0
  VPN instance     : --
  Bootfile         : 43534
  Logging          : Enable
  Conflicted address recycle interval: 1 Days 0 Hours 0 Minutes
  Address Statistic: Total       :254       Used        :1
                     Idle        :252       Expired     :2
                     Conflict    :1         Disabled    :0

--------------------------------------------------------------------------------
  Network section
        Start           End       Total    Used Idle(Expired) Conflict Disabled
--------------------------------------------------------------------------------
    192.168.0.1   192.168.0.254     254       1       252(2)       1     0
--------------------------------------------------------------------------------
Client-ID format as follows:
  DHCP  : mac-address                PPPoE   : mac-address
  IPSec : user-id/portnumber/vrf     PPP     : interface index
  L2TP  : cpu-slot/session-id        SSL-VPN : user-id/session-id
```

 Copyright © Huawei Technologies Co., Ltd.

```
-------------------------------------------------------------------------------
Index           IP            Client-ID   Type      Left   Status
-------------------------------------------------------------------------------
  109   192.168.0.110                 -      -         -   Conflict
-------------------------------------------------------------------------------
```

Table 8-34 Description of the **display ip pool** command output

Item	Description
Pool-name	Name of an IP address pool. To configure the IP address pool name, run the **ip pool (system view)** command.
Pool-No	Index of the IP address pool.
Lease	Lease of the IP address pool. To configure the lease of the IP address pool, run the **lease** command.
Domain-name	Name of a domain. To configure the domain name, run the **domain-name** command.
Option-code	Value of a customized option. To configure the value, run the **option** command.
Option-subcode	Value of a customized sub-option. To configure the value, run the **option** command.
Option-type	Type of a customized option code: • ascii: indicates that the customized option code is an ASCII character string. • hex: indicates that the customized option code is a hexadecimal string. • cipher: indicates that the customized option code is a ciphertext character string. To configure the type, run the **option** command.
Option-value	Content of a customized option. To configure the content, run the **option** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
DNS-server0	Address of the DNS server. Currently, an IP address pool can be configured with up to eight DNS servers. The value 0 indicates the first DNS server address and the value 1 indicates the second DNS server address. To configure the DNS server address, run the **dns-list** command.
NBNS-server0	Address of the NetBIOS server. Currently, an address pool can be configured with up to eight NetBIOS server addresses. The value 0 indicates the first NetBIOS server address. To configure the NetBIOS server address, run the **nbns-list** command.
Netbios-type	NetBIOS type. To configure the NetBIOS type, run the **netbios-type** command.
Position	Location of the IP address pool.
Status (First)	Status of the address pool. To configure the address pool status, run the **lock (IP address pool view)** command.
Gateway-0	Gateway address. Currently, a maximum of eight gateway addresses can be configured in an IP address pool. The value 0 indicates the first gateway address. To configure the gateway address, run the **gateway-list** command.
Network	Network segment of the address pool.
Mask	Subnet mask of the address pool. To configure the subnet mask of the address pool, run the **network (IP address pool view)** command.
Bootfile	Name of the startup configuration file configured for the DHCP client. To configure the name, run the **bootfile** command.
VPN instance	Name of a VPN instance.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Logging	Status of the logging function when the DHCP server allocates IP addresses. • Enable • Disable To configure the status of the logging function, run the **logging** or **dhcp server logging** command.
Conflicted address recycle interval	The interval for the automatic reclaim of conflicting IP addresses in the address pool. To configure the status of the logging function, run the **conflict auto-recycle interval** **day** *day* [**hour** *hour* [**minute** *minute*]] command.
Address Statistic	Statistics about IP addresses in the address pool.
Start	Start IP address of the IP address pool.
End	End IP address of the IP address pool.
Total	Total number of IP addresses in the address pool. Total = Used + Idle(Expired) + Conflict + Disable
Used	Number of used IP addresses in the address pool.
Idle(Expired)	Number of idle(expired) IP addresses in the address pool.
Conflict	Number of conflicting IP addresses in the address pool.
Disabled	Number of disabled IP addresses in the address pool.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Client-ID format as follows	Client ID format: • DHCP: mac-address. The client ID format of DHCP users is a MAC address. • PPPoE: mac-address. The client ID format of PPPoE users is a MAC address. • IPSec: user-id/portnumber/vrf. The client ID format of IPSec users is a user ID, port number, or VPN index. • PPP: interface index. The client ID format of PPP users is an interface index. • L2TP: cpu-slot/session-id. The client ID format of L2TP users is a CPU ID-slot ID or session ID. • SSL-VPN: user-id/session-id. The client ID format of SSL-VPN users is a user ID or session ID.
Index	Index.
IP	IP address.
Client-ID	DHCP client ID.
Type	DHCP client type. The types include DHCP, PPPoE, IPSec, PPP, L2TP, and SSL-VPN.
Left	Remaining lease of an IP address. When the result of the calculation formula ([**Lease** - **Left**]/**Lease**) is 50% or 87.5%, the DHCP client sends a DHCP Request message to the DHCP server to renew the lease. If the renewal succeeds, the value of the **Left** field is recounted. If the renewal fails, the DHCP client requests an IP address again and the status of its original IP address is set to **Expired**.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Status (Second)	Status of an IP address: • Used: indicates that the IP address is used. • Idle: indicates that the IP address is idle. • Expired: indicates that the lease of the IP address expires and the IP address is idle. • Conflict: indicates that the IP address conflicts with another IP address on the network. • Disable: indicates that the IP address cannot be used. • Static-bind: indicates that the IP address is bound to a MAC address. • Static-bind used: indicates that the IP address is bound to a MAC address and used.

8.3.72 display ip pool import all

Function

The **display ip pool import all** commands displays DNS and NetBIOS configurations that a DHCP server automatically assigns to a DHCP client.

Format

display ip pool import all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **8.3.84 import all** command on the DHCP server to enable the DHCP server to automatically assign configurations of DNS server and NetBIOS server to

 Copyright © Huawei Technologies Co., Ltd.

DHCP clients. The **display ip pool import all** command displays configurations of DNS server and NetBIOS server that the DHCP server automatically assigns to DHCP clients.

Example

Display DNS and NetBIOS configurations that the DHCP server automatically assigns to the DHCP client.

```
<Huawei> display ip pool import all
--------------------------------------------------------------------------------
Parameter      Update time          Protocol  Value
--------------------------------------------------------------------------------
domain-name     -                    -         -
dns-server      -                    -         -
nbns-server     -                    -         -
--------------------------------------------------------------------------------
```

Table 8-35 Description of **display ip pool import all** command output

Item	Description
Parameter	Dynamically assigned information type: • domain-name: domain name information • dns-server: DNS server information • nbns-server: NetBIOS server information To set the dynamically assigned information type, run the **8.3.84 import all** command.
Update time	Update time of dynamically assigned information.
Protocol	Protocol type of dynamically assigned information.
Value	Contents of dynamically assigned information.

Related Topics

8.3.84 import all

8.3.41 dhcp server import all

8.3.73 display snmp-agent trap feature-name dhcp all

Function

The **display snmp-agent trap feature-name dhcp all** command displays the status of all traps on the DHCP module.

Copyright © Huawei Technologies Co., Ltd.

Format

display snmp-agent trap feature-name dhcp all

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After enabling the trap function for the DHCP module, you can run this command to check the status of all traps on the DHCP module. To enable the trap function for the DHCP module, run the **snmp-agent trap enable feature-name dhcp** command.

Prerequisites

The SNMP function has been enabled on the device. For details, see **snmp-agent**.

Example

Display the status of all traps on the DHCP module.

```
<Huawei>display snmp-agent trap feature-name dhcp all
------------------------------------------------------------------------------
Feature name: dhcp
Trap number : 15
------------------------------------------------------------------------------
Trap name                     Default switch status   Current switch status
hwNomatchSnpBindTblDhcpPktAlarm
                              off                     off
hwDhcpSnpChaddrAlarm          off                     off
hwDhcpV6PktPrefixAlarm        off                     on
hwUntrustedReplyPktAlarm      off                     off
hwDhcpPktRateAlarm            off                     on
hwSnpUserNumberAlarmIf        on                      off
hwSnpUserNumberAlarmIfResume  on                      off
hwSnpUserNumberAlarmVlan      on                      off
hwSnpUserNumberAlarmVlanResume  on
off
hwSnpUserNumberAlarmGlobal    on                      off
hwSnpUserNumberAlarmGlobalResume
                              on                      off
hwNdSnpUserNumberAlarmIf      on                      off
hwNdSnpUserNumberAlarmIfResume  on
off
hwNdSnpUserNumberAlarmGlobal  on                      off
hwNdSnpUserNumberAlarmGlobalResume

                              on                      off
```

 Copyright © Huawei Technologies Co., Ltd.

Table 8-36 Description of the **display snmp-agent trap feature-name dhcp all** command output

Item	Description
Feature name	Name of the module to which a trap belongs.
Trap number	Number of traps.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Trap name	Name of a trap. Traps on the DHCP module include: • hwNomatchSnpBindTblDhcpPktAlarm: The device sends a Huawei proprietary trap when the number of DHCP Request packets that do not match DHCP snooping binding entries and are discarded on an interface exceeds the threshold. • hwDhcpSnpChaddrAlarm: The device sends a Huawei proprietary trap when the number of discarded DHCP packets whose CHADDR field differs from the source MAC address exceeds the threshold. • hwDhcpV6PktPrefixAlarm: The device sends a Huawei proprietary trap message when the DHCPv6 prefix length exceeds the threshold. • hwUntrustedReplyPktAlarm: The device sends a Huawei proprietary trap message when the number of DHCP Reply packets discarded on an untrusted interface exceeds the threshold. • hwDhcpPktRateAlarm: The device sends a Huawei proprietary trap message when the number of discarded DHCP packets whose rate exceeds the limit exceeds the threshold. • hwSnpUserNumberAlarmIf: The device sends a Huawei proprietary trap message when the number of DHCP access users on an interface exceeds the upper threshold. • hwSnpUserNumberAlarmIfResume: The device sends a Huawei proprietary trap message when the number of DHCP access users on an interface falls below the lower threshold. • hwSnpUserNumberAlarmVlan: The device sends a Huawei proprietary trap message when the number of DHCP access users in a VLAN exceeds the upper threshold. • hwSnpUserNumberAlarmVlanResume: The device sends a Huawei proprietary trap message when the number of DHCP access users in a VLAN falls below the lower threshold. • hwSnpUserNumberAlarmGlobal: The device sends a Huawei proprietary trap message when the number of DHCP access users on the device exceeds the upper threshold. • hwSnpUserNumberAlarmGlobalResume: The device sends a Huawei proprietary trap message when the number of DHCP access users on the device falls below the lower threshold.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• hwNdSnpUserNumberAlarmIf: The device sends a Huawei proprietary trap message when the number of ND access users on an interface exceeds the upper threshold. • hwNdSnpUserNumberAlarmIfResume: The device sends a Huawei proprietary trap message when the number of ND access users on an interface falls below the lower threshold. • hwNdSnpUserNumberAlarmGlobal: The device sends a Huawei proprietary trap message when the number of ND access users on the device exceeds the upper threshold. • hwNdSnpUserNumberAlarmGlobalResume: The device sends a Huawei proprietary trap message when the number of ND access users on the device falls below the lower threshold.
Default switch status	Default status of the trap function: • on: The trap function is enabled by default. • off: The trap function is disabled by default.
Current switch status	Trap status: • on: The trap is enabled. • off: The trap is disabled.

Related Topics

8.3.106 snmp-agent trap enable feature-name dhcp

8.3.74 display snmp-agent trap feature-name mid_am all

Function

The **display snmp-agent trap feature-name mid_am all** command displays the status of all traps for the AM module.

Format

display snmp-agent trap feature-name mid_am all

Parameters

None

Views

All views

Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After enabling the trap function for the AM module, you can run this command to check the status of all traps for the AM module. You can run the **snmp-agent trap enable feature-name mib_am** command to enable the trap function for the AM module.

Prerequisites

SNMP has been enabled on the device. You can enable SNMP using the **snmp-agent** command.

Example

Display the status of all traps for the AM module.

```
<Huawei>display snmp-agent trap feature-name mid_am all
------------------------------------------------------------------------------
Feature name: MID_AM
Trap number : 2
------------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
hwUsedIPReachThreshold          on                      on
hwUsedIPReachThresholdResume    on                      on
```

Table 8-37 Description of the **display snmp-agent trap feature-name mid_am all** command output

Item	Description
Feature name	Name of the module that the trap belongs to.
Trap number	Number of traps.
Trap name	Names of the traps related to the AM module, including: • hwUsedIPReachThreshold: When the number of used IP addresses in an IP address pool exceeds the upper trap threshold, the device sends a Huawei proprietary trap. • hwUsedIPReachThresholdResume: When the number of used IP addresses in an IP address pool falls below the lower trap threshold, the device sends a Huawei proprietary trap.
Default switch status	Default status of the trap function: • on: The trap function is enabled by default. • off: The trap function is disabled by default.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Current switch status	Status of the trap function: • on: The trap function is enabled. • off: The trap function is disabled.

Related Topics

8.3.107 snmp-agent trap enable feature-name mid_am

8.3.75 dns-list

Function

The **dns-list** command configures the DNS server address for the DHCP client.

The **undo dns-list** command deletes a configured DNS server address.

By default, no DNS server address is configured.

Format

IP address pool view

dns-list { *ip-address* &<1-8> | **unnumbered interface** *interface-type interface-number* }

undo dns-list { *ip-address* | **unnumbered interface** | **all** }

DHCP Option template view

dns-list *ip-address* &<1-8>

undo dns-list { *ip-address* | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies the DNS server address.	The value is in dotted decimal notation. A maximum of eight DNS server addresses can be configured. These IP addresses are separated by spaces.
unnumbered interface *interface-type interface-number*	Borrows the DNS server address obtained by the interface as the DNS server IP address.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all	Deletes all DNS server addresses.	-

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. If user hosts access hosts on the network by domain names, user hosts need to send DNS requests to the DNS server and resolve the domain name to access for communication. To connect a DHCP client to the network, configure a DHCP server address so that the DHCP server can assign both the specified DNS server address and an IP address to the client. To configure DNS server addresses for an interface address pool, run the **dhcp server dns-list** command.

Precautions

In the IP address pool view and DHCP Option template view, a device can be configured with a maximum of eight DNS server addresses respectively. The address first assigned to the clients functions as the primary address, and the other seven addresses function as secondary addresses.

Example

In the IP address pool view, set the IP address of the DNS server to 10.10.10.10.

```
<Huawei> system-view
[Huawei] ip pool global1
[Huawei-ip-pool-global1] dns-list 10.10.10.10
```

In the DHCP Option template view, set the IP address of the DNS server to 10.10.10.10.

```
<Huawei> system-view
[Huawei] dhcp option template template1
[Huawei-dhcp-option-template-template1] dns-list 10.10.10.10
```

Related Topics

8.3.83 ip pool (system view)

8.3.34 dhcp server dns-list

Copyright © Huawei Technologies Co., Ltd.

8.3.76 domain-name

Function

The **domain-name** command configures the domain name suffix for the DHCP client.

The **undo domain-name** command deletes a configured domain name suffix.

By default, no domain name suffix is configured.

Format

domain-name *domain-name*

undo domain-name

Parameters

Parameter	Description	Value
domain-name	Specifies a domain name to be assigned to a DHCP client.	The value is a string of 1 to 63 characters without spaces. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

This command applies to DHCP servers. When allocating IP addresses to the client, the DHCP server also specifies domain names for clients. Run the **domain-name** command on the DHCP server to specify a domain name. When allocating IP addresses to clients, the DHCP server also sends the domain names to the clients.

To configure a domain name for an interface address pool, run the **dhcp server domain-name (interface view)** command.

Example

In the IP address pool view, configure the domain name suffix assigned to the DHCP client as **example.com**.

Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] ip pool test
[Huawei-ip-pool-test] domain-name example.com
```

In the DHCP Option template, configure the domain name suffix assigned to the DHCP client as **huawei.com**.

```
<Huawei> system-view
[Huawei] dhcp option template template1
[Huawei-dhcp-option-template-template1] domain-name huawei.com
```

Related Topics

8.3.83 ip pool (system view)

8.3.35 dhcp server domain-name (interface view)

8.3.77 excluded-ip-address

Function

The **excluded-ip-address** command specifies the range of IP addresses that cannot be automatically assigned to clients from the address pool.

The **undo excluded-ip-address** command deletes the specified range of IP addresses that cannot be automatically assigned to clients from the address pool.

By default, all IP addresses in the address pool can be automatically assigned to clients.

Format

excluded-ip-address *start-ip-address* [*end-ip-address*]

undo excluded-ip-address *start-ip-address* [*end-ip-address*]

Parameters

Parameter	Description	Value
start-ip-address	Specifies the start IP address that cannot be automatically assigned.	The value is in dotted decimal notation.
end-ip-address	Specifies the end IP address that cannot be automatically assigned. If *end-ip-address* is not specified, only *start-ip-address* cannot be automatically assigned.	The value is in dotted decimal notation. *end-ip-address* and *start-ip-address* must be on the same network segment and *end-ip-address* must be larger than *start-ip-address*.

Views

IP address pool view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **excluded-ip-address** command applies to DHCP servers. Fixed IP addresses are allocated to some specific hosts (such as the WWW server) on the network for a long time. If these hosts' IP addresses are overlapped with IP addresses in the address pool and the DHCP server allocates these overlapped IP addresses to other hosts, IP address conflicts may occur. To prevent the IP address conflict, you need to exclude these IP addresses from being automatically allocated in the address pool.

You can run the **excluded-ip-address** command to specify the IP addresses or the range of IP addresses that cannot be automatically assigned to clients in the global address pool.

You can run the **dhcp server excluded-ip-address** command to specify the IP addresses or the range of IP addresses that cannot be automatically assigned to clients in the interface address pool.

Prerequisites

Network segment addresses that can be assigned from the global address pool have been configured using the **network (address pool view)** command.

Precautions

- The excluded IP address or IP address segment must be in the local address pool.
- You do not need to exclude the gateway address configured using the **8.3.80 gateway-list** command from being automatically allocated. The device automatically adds the gateway address into the list of IP addresses that cannot be automatically allocated.

  You do not need to exclude the IP address of a server's interface connecting to a client from being automatically allocated. The device automatically sets the interface IP address to the Conflict status during address allocation.
- If you run the **excluded-ip-address** command multiple times, you can specify multiple IP addresses or IP address segments that cannot be automatically assigned to clients from the specified address pool.
- You can run the **display ip pool** command to check used IP addresses in the current address pool, and then specify unused IP addresses that cannot be automatically assigned. To exclude used IP addresses from being automatically assigned, run the **reset ip pool** command to reclaim used IP addresses first.

Example

Specify that IP addresses 10.10.10.10 to 10.10.10.20 cannot be automatically assigned to clients from the address pool **global1**.

```
<Huawei> system-view
[Huawei] ip pool global1
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-ip-pool-global1] network 10.10.10.0 mask 24
[Huawei-ip-pool-global1] excluded-ip-address 10.10.10.10 10.10.10.20
```

Related Topics

8.3.83 ip pool (system view)

8.3.92 network (IP address pool view)

8.3.36 dhcp server excluded-ip-address

8.3.78 force insert option

Function

The **force insert option** command configures a DHCP server to forcibly insert an Option field specified in the global address pool or DHCP Option template to a DHCP Response packet that it sends to a DHCP client.

The **undo force insert option** command deletes the Option field forcibly inserted to a DHCP Response packet that a DHCP server sends to a DHCP client.

By default, a DHCP server does not forcibly insert an Option field to a DHCP Response packet that it sends to a DHCP client.

Format

force insert option *code* &<1-254>

undo force insert option *code* &<1-254>

Parameters

Parameter	Description	Value
code	Specifies the code for a forcibly replied option. You can configure a DHCP server to forcibly reply one or more options.	The value is an integer that ranges from 1 to 254.

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Copyright © Huawei Technologies Co., Ltd.

When a DHCP client applies for an IP address from a DHCP server, parameters contained in the DHCP Request packet specify the options the client requires. The DHCP server inserts the required options to a DHCP Response packet.

Sometimes, the DHCP server on the existing network receives a DHCP Request packet that contains no parameter specifying the options the client requires. However, the client still wants to obtain the options configured on the global address pool. You can run the **force insert option** *code* &<1-254> command to configure the DHCP server to forcibly insert an Option field to the DHCP Response packet.

Prerequisites

The Option field has been configured in the global address pool by running the **option** *code* [**sub-option** *sub-code*] { **ascii** *ascii-string* | **hex** *hex-string* | **cipher** *cipher-string* | **ip-address** *ip-address* &<1-8> } command in the global address pool view.

Example

Configure a DHCP server to forcibly insert Option 4 to a DHCP Response packet in the address pool **pool1**.

```
<Huawei> system-view
[Huawei] ip pool pool1
[Huawei-ip-pool-pool1] option 4 hex 11 22
[Huawei-ip-pool-pool1] force insert option 4
```

Configure a DHCP server to forcibly insert Option 4 to a DHCP Response packet in the DHCP Option template **template1**.

```
<Huawei> system-view
[Huawei] dhcp option template template1
[Huawei-dhcp-option-template-template1] option 4 hex 11 22
[Huawei-dhcp-option-template-template1] force insert option 4
```

Related Topics

8.3.83 ip pool (system view)

8.3.94 option

8.3.20 dhcp option template

8.3.79 gateway (DHCP server group view)

Function

The **gateway** command specifies an egress gateway address of the DHCP server in the DHCP server group view.

The **undo gateway** command restores the default setting.

By default, no egress gateway address is specified.

Format

gateway *ip-address*

undo gateway

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of an egress gateway.	The value is in dotted decimal notation.

Views

DHCP server group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP relay agents. If a DHCP server and its DHCP relay agent are on different network segments, you can run the **gateway** command to specify an egress gateway address for the DHCP relay agent. In this way, the DHCP relay agent can communicate with the DHCP server. Run the **gateway-list** command to configure an egress gateway for the DHCP server.

Precautions

- If an egress gateway is not configured for a DHCP relay agent using the **gateway** command, the DHCP relay agent uses the interface address as the gateway address to communicate with the DHCP server.
- When two router devices function as the DHCP server and DHCP relay agent respectively, they must use the same egress gateway address.

Example

Specify the egress gateway address of the server group **myServers** as 10.10.10.1.

```
<Huawei> system-view
[Huawei] dhcp server group myServers
[Huawei-dhcp-server-group-myServers] gateway 10.10.10.1
```

8.3.80 gateway-list

Function

The **gateway-list** command configures the egress gateway address for the DHCP client.

The **undo gateway-list** command deletes a configured egress gateway address.

By default, no egress gateway address is configured.

Copyright © Huawei Technologies Co., Ltd.

Format

gateway-list *ip-address* &<1-8>

undo gateway-list { *ip-address* | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies an egress gateway address.	The value is in dotted decimal notation.
all	Deletes all gateway addresses.	-

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. If a DHCP server and its client are on different network segments, you can run the **gateway-list** command to specify an egress gateway address. In this way, the DHCP server and client can communicate with each other. Then the DHCP server can assign both an IP address and the specified egress gateway address to the client. You can configure multiple gateways in a global address pool to load balance traffic and improve network reliability.

Run the **8.3.79 gateway (DHCP server group view)** command to configure an egress gateway for a DHCP relay agent.

Configuration Impact

If a gateway address is configured on the DHCP server, a DHCP client obtains the gateway address from the DHCP server and automatically generates a default route to the gateway address. If you run the **option121** command on the DHCP server to allocate classless static routes to DHCP clients, the DHCP client uses an allocated classless static route and does not automatically generate a default route to the gateway address.

Precautions

In the IP address pool view and DHCP Option template view, the Router can be configured with a maximum of eight egress gateway addresses respectively. These gateway addresses cannot be subnet broadcast addresses.

 Copyright © Huawei Technologies Co., Ltd.

Example

In the IP address pool view, set the egress gateway address for the DHCP client to 10.1.1.1.

```
<Huawei> system-view
[Huawei] ip pool global1
[Huawei-ip-pool-global1] gateway-list 10.1.1.1
```

In the DHCP Option template, set the egress gateway address for the DHCP client to 10.1.1.1.

```
<Huawei> system-view
[Huawei] dhcp option template template1
[Huawei-dhcp-option-template-template1] gateway-list 10.1.1.1
```

Related Topics

8.3.83 ip pool (system view)

8.3.20 dhcp option template

8.3.81 ip address bootp-alloc

Function

The **ip address bootp-alloc** command enables the BOOTP client function on an interface.

The **undo ip address bootp-alloc** command disables the BOOTP client function from an interface.

By default, the BOOTP client function is disabled on an interface.

Format

ip address bootp-alloc [**unicast**]

undo ip address bootp-alloc

Parameters

None

Parameter	Description	Value
unicast	Indicates that the client requests the server to unicast response packets to the client.	-

Views

Interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

DHCP is developed based on the BOOTP protocol. The device supports both DHCP and BOOTP and allows hosts to obtain IP addresses by BOOTP.

To enable an interface to obtain IP addresses using BOOTP, you can enable the BOOTP client function on the interface. A BOOTP client requests for an IP address from the server using BOOTP. The BOOTP client has two functions:

- Sends BOOTP Request messages to the server.
- Processes BOOTP Reply messages from the server.

To obtain an IP address, the BOOTP client sends a BOOTP Request message to the server. When the server receives the BOOTP Request message, it sends a BOOTP response message to the BOOTP client. The BOOTP client obtains the assigned IP address from the response message.

Precautions

Interfaces of the Router can have IP addresses statically configured using the **ip address** command or dynamically obtain IP addresses using the **ip address bootp-alloc** command. A static IP address takes precedence over a dynamic IP address. If the interface has dynamically obtained an IP address after the **ip address bootp-alloc** command is executed, running the **undo ip address** command deletes the IP address and the **ip address bootp-alloc** command. If the interface does not obtain an IP address after the **ip address bootp-alloc** command is executed, running the **undo ip address** command does not delete the **ip address bootp-alloc** command.

Example

Enable the BOOTP client function on GE1/0/0 to obtain an IP address.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address bootp-alloc
```

8.3.82 ip address dhcp-alloc

Function

The **ip address dhcp-alloc** command enables the DHCP client function on an interface.

The **undo ip address dhcp-alloc** command disables the DHCP client function on an interface.

By default, the DHCP client function is disabled on an interface.

 Copyright © Huawei Technologies Co., Ltd.

Format

ip address dhcp-alloc [**unicast**]

undo ip address dhcp-alloc

Parameters

Parameter	Description	Value
unicast	Indicates that the client requests the server to unicast response packets.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable an interface of the Router to obtain IP addresses using DHCP, enable the DHCP client function on the interface. A BOOTP client applies for an IP address from the server using DHCP. The DHCP client has two functions:

- Sends DHCP Request messages to the server.
- Processes DHCP Reply messages from the server.

To obtain an IP address, the DHCP client sends a DHCP Request message to the server. After the server receives the DHCP Request message, it sends a DHCP response message to the DHCP client. The DHCP client obtains the assigned IP address from the response message.

Precautions

Interfaces of the device can have IP addresses statically configured using the **ip address** command or dynamically obtain IP addresses using the **ip address dhcp-alloc** command. A static IP address takes precedence over a dynamic IP address. If the interface has dynamically obtained an IP address after the **ip address dhcp-alloc** command is executed, running the **undo ip address** command deletes the IP address and the **ip address dhcp-alloc** command. If the interface does not obtain an IP address after the **ip address dhcp-alloc** command is executed, running the **undo ip address** command does not delete the **ip address dhcp-alloc** command.

Example

Enable the DHCP client function on GE1/0/0 to obtain an IP address.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address dhcp-alloc
```

8.3.83 ip pool (system view)

Function

The **ip pool** command creates a global address pool.

The **undo ip pool** command deletes a global address pool.

By default, no global address pool is created.

Format

ip pool *ip-pool-name*

undo ip pool *ip-pool-name*

Parameters

Parameter	Description	Value
ip-pool-name	Specifies the name for an IP address pool.	The value is a string of 1 to 64 characters without spaces. It can contain digits, letters, and special characters such as underscores (_), hyphens (-), and periods (.). It cannot be set to **-** or **--**.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. When configuring a DHCP server, run the **ip pool (system view)** command in the system view to create a global IP address pool and set parameters for the global IP address pool, including a gateway address, the IP address lease, and a VPN instance. Then the configured DHCP server can assign IP addresses in the IP address pool to clients.

Follow-up Procedure

 Copyright © Huawei Technologies Co., Ltd.

Run the **8.3.92 network (IP address pool view)** command to specify the range of the IP addresses in the pool.

Example

Create a global address pool named **global1**.

```
<Huawei> system-view
[Huawei] ip pool global1
```

Related Topics

8.3.92 network (IP address pool view)

8.3.84 import all

Function

The **import all** command enables the device to dynamically obtain the DNS server IP address, DNS domain name suffix, and NetBIOS server IP address from the global address pool.

The **undo import all** command disables the device from dynamically obtaining the DNS server IP address, DNS domain name suffix, and NetBIOS server IP address from the global address pool.

By default, the local is disabled from dynamically obtaining the DNS server IP address, DNS domain name suffix, and NetBIOS server IP address from the global address pool.

Format

import all

undo import all

Parameters

None

Views

Global address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on the DHCP server. Run the **import all** command on the DHCP server to automatically allocate the DNS server IP address, DNS domain name suffix, and NetBIOS server IP address from the carrier to the DHCP client.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The global address pool has been created using the **ip pool (system view)** command.

Precautions

The device functions as a DHCP client to obtain the DNS server IP address, DNS domain name suffix, and NetBIOS server IP address from the carrier, and then functions as the DHCP server to allocate obtained information to DHCP clients using this command. The device cannot allocate information obtained from the carrier using other methods to clients.

Example

Enable the device to dynamically obtain configurations of DNS server and NetBIOS server from global address pool **global**.

```
<Huawei> system-view
[Huawei] ip pool global
[Huawei-ip-pool-global] import all
```

Related Topics

8.3.72 display ip pool import all

8.3.102 reset ip pool import

8.3.85 ip relay address cycle

Function

The **ip relay address cycle** command enables the DHCP server polling function on a DHCP relay agent.

The **undo ip relay address cycle** command disables the DHCP server polling function on a DHCP relay agent.

By default, DHCP server polling is disabled on a DHCP relay agent.

Format

ip relay address cycle

undo ip relay address cycle

Parameters

None

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

This command applies to DHCP relay agents. When multiple DHCP server addresses are configured on a DHCP relay agent, the DHCP relay agent forwards DHCP Discover messages to all servers by default. As a result, DHCP servers need to process a large number of messages, leading to heavy loads of servers. To solve this problem, configure the **ip relay address cycle** command. After this command is configured, the DHCP relay agent forwards a received DHCP Discover message to one DHCP server at a time, and forwards the DHCP Discover message to a different DHCP server each time it receives the message. Multiple DHCP servers then can allocate the same number of IP addresses, implementing load balancing among DHCP servers.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command.

Example

Enable DHCP server polling on the router in the system view.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] ip relay address cycle
```

Related Topics

8.3.18 dhcp enable

8.3.86 ip route dhcp

Function

The **ip route dhcp** command configures a routing entry delivered by the DHCP server to a DHCP client.

The **undo ip route dhcp** command cancels the configuration.

By default, no routing entry is delivered by the DHCP server to a DHCP client.

Format

ip route *ip-address* { *mask* | *mask-length* } *interface-type interface-number* **dhcp** [*preference-value*]

undo ip route *ip-address* { *mask* | *mask-length* } *interface-type interface-number* **dhcp** [*preference-value*]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip-address	Specifies the destination IP address.	The value is in dotted decimal notation.
mask	Specifies the mask of the IP address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length. The 32-bit mask is represented by consecutive 1s, and the mask in dotted decimal notation can be replaced by the mask length.	The value is an integer that ranges from 0 to 32.
interface-type interface-number	Specifies the type and number of the interface that forwards packets.	-
dhcp	Indicates that the DHCP client obtains routing entries using DHCP.	-
preference-value	Specifies the priority of the routing protocol.	The value is an integer that ranges from 1 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The **ip route dhcp** command is used on DHCP clients. After the **ip route** *ip-address* { *mask* | *mask-length* } *interface-type interface-number* **dhcp** [*preference-value*] command is run, a route with the gateway address as the next-hop IP address is automatically generated when a DHCP client obtains an IP address from the DHCP server through a DHCP request.

Example

Configure a routing entry to be obtained in DHCP mode on the DHCP client, and specify GE1/0/0 as the outbound interface for forwarding packets and 30 as the routing protocol priority.

```
<Huawei> system-view
[Huawei] ip route 10.1.1.1 24 gigabitethernet 1/0/0 dhcp 30
```

 Copyright © Huawei Technologies Co., Ltd.

8.3.87 lease

Function

The **lease** command sets the lease for IP addresses in a global IP address pool.

The **undo lease** command restores the default lease of IP addresses in a global IP address pool.

By default, the lease of IP addresses is one day.

Format

lease { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }

undo lease

Parameters

Parameter	Description	Value
day *day*	Specifies the number of days in the IP address lease.	The value is an integer that ranges from 0 to 999. The default value is 1.
hour *hour*	Specifies the number of hours in the IP address lease.	The value is an integer that ranges from 0 to 23. The default value is 0.
minute *minute*	Specifies the number of minutes in the IP address lease.	The value is an integer that ranges from 0 to 59. The default value is 0.
unlimited	Indicates that the IP address lease is unlimited.	-

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. To meet different client requirements, DHCP supports dynamic, automatic, and static address assignment.

Different hosts require different IP address leases. For example, if some hosts such as a DNS server need to use certain IP addresses for a long time, run the **lease**

 Copyright © Huawei Technologies Co., Ltd.

command to set the IP address lease of the current global address pool to **unlimited**. If some hosts such as a portable computer just need to use temporary IP addresses, run the **lease** command to set the IP address lease of the current global address pool to the required time so that the expired IP addresses can be released and assigned to other clients.

When a DHCP client starts and 50% or 87.5% of its IP address lease has passed, the DHCP client sends a DHCP Request message to the DHCP server to renew the lease.

- If the IP address can be assigned to the client, the DHCP server informs the client that the IP address lease can be renewed.
- If the IP address can no longer be assigned to the client, the DHCP server informs the client that the IP address lease cannot be renewed. The client needs to request for another IP address.

You can run the **8.3.71 display ip pool** command to view information about the IP address lease. The values of the **lease** and **left** fields in the command output indicate the configured lease time and remaining lease time, respectively.

Prerequisites

A global IP address pool has been created using the **8.3.83 ip pool (system view)** command and the DHCP server function is enabled using the **dhcp enable** command.

Precautions

Different IP address leases can be specified for different global address pools on a DHCP server. In a global address pool, all addresses have the same lease.

To specify the IP address lease for an interface address pool, run the **dhcp server lease** command.

If the IP address lease of an address pool is changed using this command, newly assigned IP addresses use the new IP address lease. IP addresses assigned before the change still use the original IP address lease before the lease is updated, and use the new lease after the lease is updated.

Example

Set the lease of a global address pool **global1** to 2 days 2 hours and 30 minutes.

```
<Huawei> system-view
[Huawei] ip pool global1
[Huawei-ip-pool-global1] lease day 2 hour 2 minute 30
```

Related Topics

8.3.83 ip pool (system view)

8.3.88 lock (IP address pool view)

Function

The **lock** command locks an IP address pool.

Copyright © Huawei Technologies Co., Ltd.

The **undo lock** restores the default configuration.

By default, no IP address pool is locked.

Format

lock [**track nqa** *admin-name test-name*]

undo lock

Parameters

Parameter	Description	Value
track nqa *admin-name test-name*	Specifies the NQA test instance to be associated with the IP address pool. • *admin-name*: specifies the name of the administrator for the NQA test instance. • *test-name*: specifies the name of the NQA test instance.	The value is a string of 1 to 32 case-sensitive characters without any space.

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **lock** command is run, the specified IP address pool is locked and IP addresses in this address pool cannot be assigned to clients. When a DHCP server needs to be redeployed, you need to migrate address pools on the DHCP server to another DHCP server on the live network. To retain the addresses that have been assigned to clients from a global address pool, run the **lock** command to lock the global address pool. When new users get online after the address pool migration, they apply for IP addresses from a new address pool.

After **track nqa** *admin-name test-name* is specified, the device can function as the backup DHCP server, and its IP address pool is associated with NQA test instances to check the DHCP server status (including the link and DHCP server function). This improves network reliability. When the DHCP server is working properly, the IP address pool is locked, and users obtain IP addresses through the DHCP server. When NQA detects that the DHCP server is faulty, the IP address pool is unlocked and assigns IP addresses to newly online users. When NQA detects that the DHCP

 Copyright © Huawei Technologies Co., Ltd.

server fault is rectified, the IP address pool is locked again, and newly online users obtain IP addresses through the DHCP server.

An IP address pool can be associated with NQA test instances of the DHCP and ICMP types. According to the test mechanism, NQA test instances of the DHCP type are used to test whether the DHCP server function is normal; those of the ICMP type are used to test whether routes to the DHCP server are reachable. You can select one NQA test instance type based on the site requirements.

Prerequisites

Before specifying the NQA test instance to be associated with the IP address pool using **track nqa** *admin-name test-name*, perform the following operations and start the NQA test instance.

- Configuring and starting an NQA test instance of the DHCP type
  a. Run the **system-view** command to enter the system view.
  b. Run the **nqa test-instance** *admin-name test-name* command to create an NQA test instance and enter the test instance view.
  c. Run the **test-type dhcp** command to configure the test type to DHCP.
  d. Run the **source-interface** *interface-type interface-number* command to specify the source interface for sending DHCP packets.
  e. Run the **frequency** *interval* command to set the automatic test interval for the NQA test instance.
  f. Run the **start** command to start the NQA test instance.

     An NQA test instance can be started immediately, at a specified time, or after a specified delay.

     - Run the **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }] command to start the test instance immediately.
     - Run the **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }] command to start the test instance at a specified time.
     - Run the **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }] command to start the test instance after a specified delay.
- Configuring and starting an NQA test instance of the ICMP type
  a. Run the **system-view** command to enter the system view.
  b. Run the **nqa test-instance** *admin-name test-name* command to create an NQA test instance and enter the test instance view.
  c. Run the **test-type icmp** command to configure the test type to ICMP.
  d. Run the **destination-address ipv4** *ipv4-address* command to configure the destination IP address.
  e. Run the **frequency** *interval* command to set the automatic test interval for the NQA test instance.
  f. Run the **start** command to start the NQA test instance.

 Copyright © Huawei Technologies Co., Ltd.

An NQA test instance can be started immediately, at a specified time, or after a specified delay.

- Run the **start now** [**end** { **at** [*yyyy/mm/dd*] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } }] command to start the test instance immediately.
- Run the **start at** [*yyyy/mm/dd*] *hh:mm:ss* [**end** { **at** [*yyyy/mm/dd*] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } }] command to start the test instance at a specified time.
- Run the **start delay** { **seconds** *second* | *hh:mm:ss* } [**end** { **at** [*yyyy/mm/dd*] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } }] command to start the test instance after a specified delay.

Precautions

An IP address pool can be associated to only one NQA test instance. If you run the **lock** [**track nqa** *admin-name test-name*] command multiple times, the last configuration takes effect.

When the NQA test instance type is not DHCP and ICMP, the association between the IP address pool and NQA do not take effect. In this case, the IP address pool is locked.

Example

Lock the IP address pool **global1**.

```
<Huawei> system-view
[Huawei] ip pool global1
[Huawei-ip-pool-global1] lock
```

Configure an NQA test instance of the DHCP type and check whether the IP address pool **global1** is locked according to the NQA detection result.

```
<Huawei> system-view
[Huawei] nqa test-instance admin test
[Huawei-nqa-admin-test] test-type dhcp
[Huawei-nqa-admin-test] source-interface gigabitethernet 1/0/0
[Huawei-nqa-admin-test] start now
[Huawei-nqa-admin-test] quit
[Huawei] ip pool global1
[Huawei-ip-pool-global1] lock track nqa admin test
```

Related Topics

8.3.83 ip pool (system view)

8.3.89 logging (IP address pool view)

Function

The **logging** command enables the logging function during IP address allocation of the DHCP server in the IP address pool view.

The **undo logging** command disables the logging function during IP address allocation of the DHCP server in the IP address pool view.

Copyright © Huawei Technologies Co., Ltd.

By default, the logging function during IP address allocation of the DHCP server is disabled.

Format

logging [**allocation-fail** | **allocation-success** | **release** | **renew-fail** | **renew-success** | **detect-conflict** | **recycle-conflict**] *

undo logging [**allocation-fail** | **allocation-success** | **release** | **renew-fail** | **renew-success** | **detect-conflict** | **recycle-conflict**] *

Parameters

Parameter	Description	Value
allocation-fail	Displays logs when address allocation fails.	-
allocation-success	Displays logs when address allocation succeeds.	-
release	Displays logs when addresses are released.	-
renew-fail	Displays logs when address lease renewal fails.	-
renew-success	Displays logs when address lease renewal succeeds.	-
detect-conflict	Displays logs when address conflict occurs.	-
recycle-conflict	Displays logs when conflicting addresses are reclaimed.	-

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on a DHCP server. When the DHCP server allocates IP addresses to clients, it records address allocation information to facilitate routine maintenance and fault location. After the logging function during IP address allocation of the DHCP server is configured using the **logging** command, the DHCP server records logs about address allocation, conflict, lease renewal, and release.

Run the **display ip pool name** *ip-pool-name* command to check the status of the logging function during IP address allocation of the DHCP server.

Prerequisites

The global address pool has been created using the **ip pool (system view)** command.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

- With this logging function enabled, if a large number of DHCP clients request IP addresses from the DHCP server, the server frequently records logs. The server performance may therefore be affected.
- IP address allocation logs are recorded in the AM module. To view log information, the information center must be enabled. In addition, default settings for log output vary depending on various factors including the log level and output direction. For details, see Information Center Configuration.

  For example, the level of logs indicating that an IP address is successfully allocated, an IP address is successfully renewed, and an IP address is successfully released is informational, and these logs are not recorded in the log buffer by default. You can run the **info-center source AM channel 4 log level informational** command to change the level of the logs to be recorded in the log buffer. You can then run the **display logbuffer** command to check the preceding logs.

Example

Enable the logging function during IP address allocation of the DHCP server in the IP address pool **pool1**.

```
<Huawei> system-view
[Huawei] ip pool pool1
[Huawei-ip-pool-pool1] logging
```

8.3.90 nbns-list

Function

The **nbns-list** command configures the NetBIOS server address for the DHCP client.

The **undo nbns-list** command deletes a configured NetBIOS server address.

By default, no NetBIOS server address is configured.

Format

nbns-list *ip-address* &<1-8>

undo nbns-list { *ip-address* | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a NetBIOS server.	The value is in dotted decimal notation. A maximum of eight NetBIOS server addresses can be configured. These IP addresses are separated by spaces.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all	Deletes all NetBIOS server addresses.	-

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. Before hosts communicate with each other, a NetBIOS server needs to resolve the accessedNetBIOS hostname to an IP address. To enable hosts to communicate with each other, run the **nbns-list** command to configure NetBIOS server addresses. When assigning IP addresses to clients, a DHCP server also assigns the configured NetBIOS server addresses to clients. To configure NetBIOS server addresses for an interface address pool, run the **dhcp server nbns-list** command.

Precautions

In the IP address pool view and DHCP Option template view, a device can be configured with a maximum of eight NetBIOS server addresses respectively. The first assigned address functions as the primary address, and the other seven addresses function as secondary addresses.

Example

In the IP address pool view, set the IP address of the NetBIOS server to 192.168.1.1.

```
<Huawei> system-view
[Huawei] ip pool global1
[Huawei-ip-pool-global1] nbns-list 192.168.1.1
```

In the DHCP Option template view, set the IP address of the NetBIOS server to 10.1.1.1.

```
<Huawei> system-view
[Huawei] dhcp option template template1
[Huawei-dhcp-option-template-template1] nbns-list 10.1.1.1
```

Related Topics

8.3.83 ip pool (system view)

8.3.46 dhcp server nbns-list

8.3.20 dhcp option template

Copyright © Huawei Technologies Co., Ltd.

8.3.91 netbios-type

Function

The **netbios-type** command configures the NetBIOS node type for the DHCP client.

The **undo netbios-type** command deletes a configured NetBIOS node type.

By default, no NetBIOS node type for the DHCP client is configured.

Format

netbios-type { **b-node** | **h-node** | **m-node** | **p-node** }

undo netbios-type

Parameters

Parameter	Description	Value
b-node	Indicates a node in broadcast mode. A b-node obtains the mapping between host names and IP addresses in broadcast mode.	-
h-node	Indicates a node in hybrid mode. An h-node is a b-type node enabled with the end-to-end communication mechanism.	-
m-node	Indicates a node in mixed mode. An m-node is a p-type node with some broadcast features.	-
p-node	Indicates a node in peer-to-peer mode. A p-node obtains the mapping between host names and IP addresses by communicating with a NetBIOS server.	-

Views

IP address pool view, DHCP Option template view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. When a DHCP client uses NetBIOS for communication, its host name needs to be mapped to an IP address, and the NetBIOS node type needs to be specified for it using the **netbios-type** command. When a DHCP server assigns an IP address to clients, it also sends the specified NetBIOS node type to clients.

Prerequisites

To specify the NetBIOS node type for a client in the interface address pool, run the **dhcp server netbios-type** command.

Example

In the IP address pool view, set the NetBIOS node type for the DHCP client to **b-node**.

```
<Huawei> system-view
[Huawei] ip pool global1
[Huawei-ip-pool-global1] netbios-type b-node
```

In the DHCP Option template view, set the NetBIOS node type for the DHCP client to **b-node**.

```
<Huawei> system-view
[Huawei] dhcp option template template1
[Huawei-dhcp-option-template-template1] netbios-type b-node
```

Related Topics

8.3.83 ip pool (system view)

8.3.90 nbns-list

8.3.47 dhcp server netbios-type

8.3.92 network (IP address pool view)

Function

The **network** command sets a network segment address for a global address pool.

The **undo network** command restores the default network segment address.

By default, no network segment address is specified.

Format

network *ip-address* [**mask** { *mask* | *mask-length* }]

undo network

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip-address	Specifies a network segment address.	The value is in dotted decimal notation.
mask	Specifies the mask of the network segment address. If this parameter is not specified, the natural mask is used.	-
mask	Specifies the mask of the network segment address.	The value is in dotted decimal notation.
mask-length	Specifies the network mask length of the DHCP server.	The value is an integer that ranges from 0 to 32.

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. Before a DHCP server assigns IP addresses to clients from a global address pool, run the **network** command to set a network segment address for the global address pool so that the DHCP server can select and assign IP addresses on this network segment to clients. When a DHCP server assigns an IP address to the client from the interface address pool, the network segment of the interface IP address is that of the interface address pool.

Precautions

Each IP address pool can be configured with only one network segment. If the system needs multiple address segments, multiple IP address pools are required.

The size of an address pool can be controlled by setting the mask length. The mask length is in reverse proportion to the address pool size.

When configuring an address pool, ensure that IP addresses on the network address segment must be class A, B, or C IP addresses, and the mask cannot be set to 0, 1, 31, or 32.

The size of the IP address pool cannot be larger than 64K.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the network segment address of the IP address pool **global1** to 192.168.1.0 and mask length to 24.

```
<Huawei> system-view
[Huawei] ip pool global1
[Huawei-ip-pool-global1] network 192.168.1.0 mask 24
```

Related Topics

8.3.83 ip pool (system view)

8.3.93 next-server

Function

The **next-server** command configures the IP address of a server for the DHCP client after the client automatically obtains the IP address.

The **undo next-server** command deletes a configured IP address of a server for the DHCP client after the client automatically obtains the IP address.

By default, no IP address of a server is configured for the DHCP client after the client automatically obtains the IP address.

Format

next-server *ip-address*

undo next-server

Parameters

Parameter	Description	Value
ip-address	Specifies a server IP address.	The value is in dotted decimal notation.

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **next-server** command is used on DHCP servers. When assigning a client an IP address, a DHCP server can also assign the client an IP address of the server that provides network services for the client. For example, after obtaining IP addresses,

 Copyright © Huawei Technologies Co., Ltd.

clients such as IP phones need parameters such as the startup configuration file to work normally. You can run the **next-server** command to specify the server address used after a client obtains an IP address. The client then requests the configuration parameters from the specified server after obtaining an IP address.

If users use addresses in the interface address pool, run the **dhcp server next-server** command to specify the DHCP server IP address. If users use addresses in the global address pool, run the **next-server** command to specify the DHCP server IP address.

Precautions

- Only one IP address of a server that provides network services can be configured in each IP address pool view or DHCP Option template view. If the system needs multiple IP addresses of servers that provide network services, configure multiple IP address pools or DHCP Option templates.
- If you run the **next-server** command multiple times, only the latest configuration takes effect.

Example

In the IP address pool view, set the IP address of a server for the DHCP client after the client automatically obtains the IP address to 10.1.2.2.

```
<Huawei> system-view
[Huawei] ip pool global1
[Huawei-ip-pool-global1] next-server 10.1.2.2
```

In the DHCP Option template view, set the IP address of a server for the DHCP client after the client automatically obtains the IP address to 10.1.2.2.

```
<Huawei> system-view
[Huawei] dhcp option template template1
[Huawei-dhcp-option-template-template1] next-server 10.1.2.2
```

Related Topics

8.3.48 dhcp server next-server

8.3.20 dhcp option template

8.3.94 option

Function

The **option** command configures the user-defined option that a DHCP server assigns to a DHCP client.

The **undo option** command deletes the user-defined option that a DHCP server assigns to a DHCP client.

By default, no user-defined option that a DHCP server assigns to a DHCP client is configured.

Format

option *code* [**sub-option** *sub-code*] { **ascii** *ascii-string* | **hex** *hex-string* | **cipher** *cipher-string* | **ip-address** *ip-address* &<1-8> }

undo option [*code* [**sub-option** *sub-code*]]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
code	Specifies the code for a user-defined option.	The value is an integer that ranges from 1 to 254, except values 1, 3, 6, 15, 44, 46, 50, 51, 52, 53, 54, 55, 57, 58, 59, 61, 82, 121 and 184. **NOTE** There are well-known options and customized options. For details about well-known options, see RFC 2132.
sub-option *sub-code*	Specifies the code of a user-defined sub-option.	The value is an integer that ranges from 1 to 254. For details about well-known options, see RFC 2132.
ascii *ascii-string*	Specifies the user-defined option code as an ASCII character string.	The value is a string of characters case-sensitive characters with spaces supported. If **sub-option** is not specified, the value is a string of 1 to 255 characters. If **sub-option** is specified, the value is a string of 1 to 253 characters.
hex *hex-string*	Specifies the user-defined option code as a hexadecimal string.	The value is a hexadecimal string with an even number of characters, for example, hh or hhhh. If **sub-option** is not specified, the value without spaces ranges from 1 to 254; if **sub-option** is specified, the value without spaces ranges from 1 to 252. The value can be a combination of digits (0-9) and letters (A-F and a-f).

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cipher *cipher-string*	Specifies the user-defined option code as a ciphertext character string.	The value is a string, you can enter a character string in plain text or cipher text. • The character string in plain text is a string of 1 to 64 characters. • The character string in cipher text is a string of 32 to 104. No matter whether the character string is entered in plain or cipher text, the character string is displayed in cipher text in the configuration file and in plain text in packets.
ip-address *ip-address*	Specifies the user-defined option code as an IP address.	The value is in dotted decimal notation.

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. The option field in a DHCP packet carries control information and parameters. If a DHCP server is configured with options, when a DHCP client applies for an IP address, the client can obtain the configurations in the option field of the DHCP response packet from the DHCP server. To configure user-defined options for an interface address pool, run the **dhcp server option** command.

Precautions

- To ensure accuracy, read the Request For Comments (RFC) before configuring options.
- When the password is contained in option, the **ascii** or **hex** type is insecure. Set the option type to **cipher**. A secure password should contain at least two types of the following: lowercase letters, uppercase letters, number, and

 Copyright © Huawei Technologies Co., Ltd.

special characters. In addition, the password must consist of six or more than six characters.

- Note the following if the **option** *code* [**sub-option** *sub-code*] { **ascii** *ascii-string* | **hex** *hex-string* | **cipher** *cipher-string* | **ip-address** *ip-address* &<1-8> } command is not executed for the first time:
  - If the new *code* is different from the existing *code*, both new and existing configurations take effect.
  - If the new *code* is the same as the existing *code*, the following situations may occur:
    - When a *sub-code* is specified in the existing command, the new configuration overrides the existing configuration if the new and existing *sub-code*s are the same, and both the new and existing configurations take effect if the new and existing *sub-code*s are different. If no *sub-code* is specified in the new command, the new configuration overrides the existing configuration.
    - When no *sub-code* is specified in the existing command, the new configuration overrides the existing configuration.

Example

In the global address pool **global1**, configure Option64 to 0x11 (a hexadecimal number).

```
<Huawei> system-view
[Huawei] ip pool global1
[Huawei-ip-pool-global1] option 64 hex 11
```

In the DHCP Option template **template1**, configure Option64 to 0x11 (a hexadecimal number).

```
<Huawei> system-view
[Huawei] dhcp option template template1
[Huawei-dhcp-option-template-template1] option 64 hex 11
```

Related Topics

8.3.83 ip pool (system view)

8.3.49 dhcp server option

8.3.20 dhcp option template

8.3.95 option121

Function

The **option121** command configures the classless static route for the DHCP client.

The **undo option121** command deletes a configured classless static route.

By default, no classless static route is configured.

Format

option121 ip-address { *ip-address mask-length gateway-address* } &<1-8>

undo option121 [**ip-address** *ip-address mask-length gateway-address*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip-address	Specifies the destination IP address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer that ranges from 0 to 32.
gateway-address	Specifies the gateway address of a route.	The value is in dotted decimal notation.

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **option121** command applies to only the DHCP server. The **option121** command configures Option 121 that defines a classless static route allocated to a client.

mask-length and *gateway-address* specify a classless static route. The **option121** command configures a maximum of eight classless static routes.

Precautions

- To configure multiple classless static routes, run the **option121** command repeatedly.
- The **undo option121** command will delete all classless static routes. To delete one classless static route, run the **undo option121 ip-address** *ip-address mask-length gateway-address* command.

Example

In the IP address pool view, configure classless static routes delivered by the DHCP server.

```
<Huawei> system-view
[Huawei] ip pool global1
[Huawei-ip-pool-global1] option121 ip-address 10.10.10.10 24 10.11.11.11
```

In the DHCP Option template view, configure classless static routes delivered by the DHCP server.

```
<Huawei> system-view
[Huawei] dhcp option template template1
[Huawei-dhcp-option-template-template1] option121 ip-address 10.10.10.10 24 10.11.11.11
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

8.3.83 ip pool (system view)
8.3.49 dhcp server option
8.3.20 dhcp option template

8.3.96 option184

Function

The **option184** command configures the Option 184 field for the DHCP client.

The **undo option184** command deletes a configuration in the Option 184 field.

By default, no content in the Option 184 field is configured.

Format

option184 { **as-ip** *ip-address* | **fail-over** *ip-address dialer-string* | **ncp-ip** *ip-address* | **voice-vlan** *vlan-id* }

undo option184 [**as-ip** | **fail-over** | **ncp-ip** | **voice-vlan**]

NOTE

AR109, AR109W, AR109GW-L, AR129CGVW-L do not support **voice-vlan** *vlan-id* parameter.

Parameters

Parameter	Description	Value
ncp-ip *ip-address*	Specifies the IP address of the network call processor (NCP).	The value is in dotted decimal notation.
as-ip *ip-address*	Specifies the IP address of the backup NCP.	The value is in dotted decimal notation.
fail-over *ip-address*	Specifies the IP address in the failover route.	The value is in dotted decimal notation.
dialer-string	Specifies the dialer string.	The value is a string of 1 to 64 characters.
voice-vlan *vlan-id*	Specifies the ID of a voice VLAN.	The value is an integer that ranges from 1 to 4094.

Views

IP address pool view, DHCP Option template view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

The **option184** command applies to only the DHCP server and configures Option 184 allocated by a DHCP server to a client in a global address pool.

Example

In the IP address pool view, configure the Option 184 field.

```
<Huawei> system-view
[Huawei] ip pool global1
[Huawei-ip-pool-global1] option184 as-ip 192.168.1.10
```

In the DHCP Option template view, configure the Option 184 field.

```
<Huawei> system-view
[Huawei] dhcp option template template1
[Huawei-dhcp-option-template-template1] option184 as-ip 10.10.10.10
```

Related Topics

8.3.83 ip pool (system view)

8.3.49 dhcp server option

8.3.20 dhcp option template

8.3.97 reset dhcp client statistics

Function

The **reset dhcp client statistics** command clears packet statistics about a DHCP client.

Format

reset dhcp client statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clear packet statistics about the DHCP client of the specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Copyright © Huawei Technologies Co., Ltd.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **reset dhcp client statistics** command is applicable to DHCP client. During DHCP troubleshooting, statistics about the packets sent and received within a specified period need to be checked. Therefore, before collecting packet statistics, run the **reset dhcp client statistics** command to clear the existing packet statistics. Then you can run the **display dhcp client statistics** command to check packet statistics about the DHCP client.

Precautions

The **reset dhcp client statistics** command can be run multiple times at any interval.

Example

Clear packet statistics about the DHCP client.

```
<Huawei> reset dhcp client statistics
```

Related Topics

8.3.61 display dhcp client statistics

8.3.98 reset dhcp relay statistics

Function

The **reset dhcp relay statistics** command clears message statistics on a DHCP relay agent.

Format

reset dhcp relay statistics [**server-group** *group-name*]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
server-group *group-name*	Specifies the name of a DHCP server group.	The value is a string of 1 to 32 characters without spaces. A combination of digits, letters, underscores (_), and dots (.) is allowed.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command applies to DHCP relay agents. Collecting statistics on the DHCP messages sent and received within a specified period helps you locate DHCP faults. Run the **reset dhcp relay statistics** [**server-group** *group-name*] command to clear original statistics on DHCP messages, and run the **display dhcp relay statistics** [**server-group** *group-name*] command to view packet statistics about the DHCP relay agent.

- Run the **reset dhcp relay statistics server-group** *group-name* command to clear message statistics on DHCP relay agents connected to DHCP servers in a specified DHCP server group. The DHCP server group name needs to be specified.
- Run the **reset dhcp relay statistics** command to clear message statistics on all DHCP relay agents besides DHCP relay agents connected to DHCP servers in the DHCP server group.

Precautions

The **reset dhcp relay statistics** command can be run multiple times at any interval.

Example

Clear message statistics on the DHCP relay agent.

```
<Huawei> reset dhcp relay statistics
```

Related Topics

8.3.66 display dhcp relay statistics

 Copyright © Huawei Technologies Co., Ltd.

8.3.99 reset dhcp server statistics

Function

The **reset dhcp server statistics** command clears statistics on the DHCP server.

Format

reset dhcp server statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. Collecting statistics on the DHCP messages sent and received within a specified period helps you locate DHCP faults. Run the **reset dhcp server statistics** command to clear original statistics on DHCP messages and then run the **display dhcp server statistics** to view message statistics on the DHCP server.

Precautions

The **reset dhcp server statistics** command can be run multiple times at any interval.

Example

Clear message statistics on the DHCP server.

```
<Huawei> reset dhcp server statistics
```

Related Topics

8.3.69 display dhcp server statistics

8.3.100 reset dhcp statistics

Function

The **reset dhcp statistics** command clears packet statistics about a DHCP.

 Copyright © Huawei Technologies Co., Ltd.

Format

reset dhcp statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

During DHCP troubleshooting, statistics about the packets sent and received within a specified period need to be checked. Therefore, before collecting packet statistics, run the **reset dhcp statistics** command to clear the existing packet statistics. Then you can run the **display dhcp statistics** command to view DHCP message statistics.

Example

Clear packet statistics about the DHCP.

```
<Huawei> reset dhcp statistics
```

Related Topics

8.3.70 display dhcp statistics

8.3.101 reset ip pool

Function

The **reset ip pool** command resets the IP address pool configured on the device.

Format

reset ip pool { **interface** *interface-name* | **name** *ip-pool-name* } { *start-ip-address* [*end-ip-address*] | **all** | **conflict** | **expired** | **used** }

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface *interface-name*	Specifies the name of the interface address pool to be reset, which is represented by the type and number of an interface.	The value is a string of 1 to 64 characters without spaces. A combination of digits, letters, underscores (_), and dots (.) is allowed.
name *ip-pool-name*	Specifies the name of the global address pool to be reset.	The value is a string of 1 to 64 characters without spaces. A combination of digits, letters, underscores (_), and dots (.) is allowed.
start-ip-address	Specifies the start IP address of the IP address pool to be reset.	The value is in dotted decimal notation.
end-ip-address	Specifies the end IP address of the IP address pool to be reset.	The value is in dotted decimal notation.
all	Indicates that all the IP addresses need to be reset.	-
conflict	Indicates that the conflicting IP addresses need to be reset.	-
expired	Indicates that the expired IP addresses need to be reset.	-
used	Indicates that the used IP addresses need to be reset.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

The **reset ip pool** command resets the IP addresses that cannot be released in an IP address pool. If an IP address conflict occurs because two clients use the same IP address, run the **reset ip pool** command to reset the specified IP address pool.

Precautions

If a user's IP address is within the IP address range specified when this command is run, the user cannot continue to use the IP address after this command is run, and needs to send an IP address application request again.

The address pool status cannot be restored after this command is run. Therefore, exercise caution when deciding to run this command.

Follow-up Procedure

After the address pool is set to idle, the client can obtain an IP address from the global address pool.

Example

Reset the conflicting IP addresses in the IP address pool **mypool**.

```
<Huawei> reset ip pool name mypool conflict
```

Related Topics

8.3.71 display ip pool

8.3.102 reset ip pool import

Function

The **reset ip pool import** command clears the DNS and NetBIOS configurations dynamically obtained by an address pool.

Format

reset ip pool import { **all** | **dns** | **domain-name** | **nbns** }

Parameters

Parameter	Description	Value
all	Indicates that all the configurations dynamically obtained by the address pool need to be reset.	-
dns	Indicates that the DNS configurations dynamically obtained by the address pool need to be reset.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
domain-name	Indicates that the domain-name configurations dynamically obtained by the address pool need to be reset.	-
nbns	Indicates that the NBNS configurations dynamically obtained by the address pool need to be reset.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

This command applies to DHCP servers. When the DNS and NetBIOS configurations dynamically obtained by an address pool are incorrect, run the **reset ip pool import all** command to clear the obtained configurations before recollecting the DNS and NetBIOS configurations.

Example

Clear the DNS and NetBIOS configurations dynamically obtained by an address pool.

```
<Huawei> reset ip pool import all
Warning: The network configuration parameters imported from center server will
be clean up. Continue? [Y/N]y
```

Related Topics

8.3.84 import all

8.3.41 dhcp server import all

8.3.103 section (IP address pool view)

Function

The **section** command configures the IP address segment in an IP address pool.

The **undo section** command deletes the configured IP address segment in an IP address pool.

Copyright © Huawei Technologies Co., Ltd.

By default, the IP address segment in an IP address pool is not configured.

Format

section *section-id start-address* [*end-address*]

undo section *section-id*

Parameters

Parameter	Description	Value
section-id	Specifies the ID of the address segment in the IP address pool.	The value is an integer that ranges from 0 to 255.
start-address	Specifies the start IP address of the address segment.	The value is in dotted decimal notation.
end-address	Specifies the end IP address of the address segment. **NOTE** The end IP address must be larger than the start IP address. If the end IP address is not entered, there is only one address in the address segment.	The value is in dotted decimal notation.

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

An IP address pool consists of one or more IP address segments. The IP addresses on each address segment cannot overlap.

Example

Configure an IP address segment 10.1.1.10-10.1.1.15 with the ID 0 for the IP address pool **abc**.

```
<Huawei> system-view
[Huawei] ip pool abc
[Huawei-ip-pool-abc] section 0 10.1.1.10 10.1.1.15
```

8.3.104 sip-server (IP address pool view)

 Copyright © Huawei Technologies Co., Ltd.

Function

The **sip-server** command configures the SIP server IP address assigned to a DHCP client in a global address pool.

The **undo sip-server** command deletes the configured SIP server IP address assigned to a DHCP client in a global address pool.

By default, the SIP server IP address assigned to a DHCP client in a global address pool is not configured.

Format

sip-server { **ip-address** *ip-address* &<1-2> | **list** *domain-name* &<1-2> }

undo sip-server

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies an IP address for the SIP server.	The value is in dotted decimal notation.
list *domain-name*	Specifies the domain name of the SIP server.	The value is a string of 1 to 63 characters.

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to the DHCP server. To enable DHCP clients to normally access the Internet, the DHCP server needs to specify the SIP server IP address in the address pool when assigning IP addresses to the clients.

Precautions

- A maximum of two SIP server addresses can be configured in each address pool. The first assigned address functions as the primary address, and the other address functions as a secondary address.
- Before specifying the IP address or name for a SIP server, ensure that the SIP server exists.
- If you run this command repeatedly, the latest configuration overrides the previous ones.

 Copyright © Huawei Technologies Co., Ltd.

Example

Specify 192.168.1.1 as the IP address of the SIP server when addresses in the global address pool **global1** are assigned to clients.

```
<Huawei> system-view
[Huawei] ip pool global1
[Huawei-ip-pool-global1] sip-server ip-address 192.168.1.1
```

8.3.105 sname

Function

The **sname** command configures the name of the server from which the DHCP client obtains the startup configuration file.

The **undo sname** command deletes the configured name of the server from which the DHCP client obtains the startup configuration file.

By default, no name is configured for the server from which the DHCP client obtains the startup configuration file.

Format

sname *sname*

undo sname

Parameters

Parameter	Description	Value
sname	Specifies the name of the server where the DHCP client obtains the startup configuration file.	The value is a string of 1 to 63 case-sensitive characters without spaces.

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Besides assigning IP addresses, a DHCP server can also provide the required network configuration parameters, such as the startup configuration file name for the DHCP client. After the name of the server from which the DHCP client obtains the startup configuration file is configured using the **sname** command, the DHCP client obtains the startup configuration file from this server.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

Ensure that the route between the DHCP client and the file server from which the DHCP client obtains the startup configuration file is reachable.

Example

In the IP address pool view, configure the name of the server from which the DHCP client obtains the startup configuration file as **example**.

```
<Huawei> system-view
[Huawei] ip pool p1
[Huawei-ip-pool-p1] sname example
```

In the DHCP Option template view, configure the name of the server from which the DHCP client obtains the startup configuration file as **Huawei**.

```
<Huawei> system-view
[Huawei] dhcp option template template1
[Huawei-dhcp-option-template-template1] sname Huawei
```

Related Topics

8.3.83 ip pool (system view)

8.3.20 dhcp option template

8.3.106 snmp-agent trap enable feature-name dhcp

Function

The **snmp-agent trap enable feature-name dhcp** command enables the trap function for the DHCP module.

The **undo snmp-agent trap enable feature-name dhcp** command disables the trap function for the DHCP module.

For details about whether the trap function for the DHCP module is enabled or disabled by default, see **8.3.73 display snmp-agent trap feature-name dhcp all**.

Format

snmp-agent trap enable feature-name dhcp [**trap-name** { **hwdhcppktratealarm** | **hwdhcpsnpchaddralarm** | **hwdhcpv6pktprefixalarm** | **hwndsnpusernumberalarmglobal** | **hwndsnpusernumberalarmglobalresume** | **hwndsnpusernumberalarmif** | **hwndsnpusernumberalarmifresume** | **hwnomatchsnpbindtbldhcppktalarm** | **hwsnpusernumberalarmglobal** | **hwsnpusernumberalarmglobalresume** | **hwsnpusernumberalarmif** | **hwsnpusernumberalarmifresume** | **hwsnpusernumberalarmvlan** | **hwsnpusernumberalarmvlanresume** | **hwuntrustedreplypktalarm** }]

undo snmp-agent trap enable feature-name dhcp [**trap-name** { **hwdhcppktratealarm** | **hwdhcpsnpchaddralarm** | **hwdhcpv6pktprefixalarm** | **hwndsnpusernumberalarmglobal** | **hwndsnpusernumberalarmglobalresume** | **hwndsnpusernumberalarmif** | **hwndsnpusernumberalarmifresume** | **hwnomatchsnpbindtbldhcppktalarm** | **hwsnpusernumberalarmglobal** | **hwsnpusernumberalarmglobalresume** | **hwsnpusernumberalarmif** | **hwsnpusernumberalarmifresume** | **hwsnpusernumberalarmvlan** | **hwsnpusernumberalarmvlanresume** | **hwuntrustedreplypktalarm** }]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
trap-name	Enables or disables the trap function for a specified event of the DHCP module.	-
hwdhcppktratealarm	Enables the device to send a Huawei proprietary trap when the number of discarded DHCP packets whose rate exceeds the limit exceeds the threshold.	-
hwdhcpsnpchaddra-larm	Enables the device to send a Huawei proprietary trap when the number of discarded DHCP packets whose CHADDR field differs from the source MAC address exceeds the threshold.	-
hwdhcpv6pktprefixalarm	Enables the device to send a Huawei proprietary trap when the DHCPv6 prefix length exceeds the threshold.	-
hwndsnpusernumbera-larmglobal	Enables the device to send a Huawei proprietary trap when the number of ND access users on the device exceeds the upper threshold.	-
hwndsnpusernumbera-larmglobalresume	Enables the device to send a Huawei proprietary trap when the number of ND access users on the device falls below the lower threshold.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwndsnpusernumberalarmif	Enables the device to send a Huawei proprietary trap when the number of ND access users on an interface exceeds the upper threshold.	-
hwndsnpusernumberalarmifresume	Enables the device to send a Huawei proprietary trap when the number of ND access users on an interface falls below the lower threshold.	-
hwnomatchsnpbindtbldhcppktalarm	Enables the device to send a Huawei proprietary trap when the number of DHCP Request packets that do not match DHCP snooping binding entries and are discarded on an interface exceeds the threshold.	-
hwsnpusernumberalarmglobal	Enables the device to send a Huawei proprietary trap when the number of DHCP access users on the device exceeds the upper threshold.	-
hwsnpusernumberalarmglobalresume	Enables the device to send a Huawei proprietary trap when the number of DHCP access users on the device falls below the lower threshold.	-
hwsnpusernumberalarmif	Enables the device to send a Huawei proprietary trap when the number of DHCP access users on an interface exceeds the upper threshold.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwsnpusernumberalar-mifresume	Enables the device to send a Huawei proprietary trap when the number of DHCP access users on an interface falls below the lower threshold.	-
hwsnpusernumbera-larmvlan	Enables the device to send a Huawei proprietary trap when the number of DHCP access users in a VLAN exceeds the upper threshold.	-
hwsnpusernumbera-larmvlanresume	Enables the device to send a Huawei proprietary trap when the number of DHCP access users in a VLAN falls below the lower threshold.	-
hwuntrustedreplypkta-larm	Enables the device to send a Huawei proprietary trap when the number of DHCP Reply packets discarded on an untrusted interface exceeds the threshold.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

After the trap function is enabled, the device generates traps during operation and sends the traps to the NMS through the SNMP module. If the trap function is disabled, the device does not generate traps and the SNMP module does not send traps to the NMS.

You can specify **snmp-agent** to enable the trap function for one or more events.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

For traps that are enabled by default, the device has the trap suppression function configured and does not report traps within 10 minutes.

Example

Enable the trap function for hwdhcppktratealarm of the DHCP module.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name dhcp trap-name hwdhcppktratealarm
```

Related Topics

8.3.73 display snmp-agent trap feature-name dhcp all

8.3.107 snmp-agent trap enable feature-name mid_am

Function

The **snmp-agent trap enable feature-name mid_am** command enables the trap function for the AM module.

The **undo snmp-agent trap enable feature-name mid_am** command disables the trap function for the AM module.

By default, the trap function is enabled for the AM module.

Format

snmp-agent trap enable feature-name mid_am [**trap-name** { **hwusedipreachthreshold** | **hwusedipreachthresholdresume** }]

undo snmp-agent trap enable feature-name mid_am [**trap-name** { **hwusedipreachthreshold** | **hwusedipreachthresholdresume** }]

Parameters

Parameter	Description	Value
trap-name	Enables or disables the trap function for the specified event of the AM module.	-
hwusedipreachthres-hold	Enables the function of sending Huawei proprietary traps when the number of used IP addresses in an IP address pool exceeds the upper trap threshold.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwusedipreachthre-sholdresume	Enables the function of sending Huawei proprietary traps when the number of used IP addresses in an IP address pool falls below the lower trap threshold.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

After the trap function is enabled, the device generates traps during operation and sends the traps to the NMS through the SNMP module. If the trap function is disabled, the device does not generate traps and the SNMP module does not send traps to the NMS.

You can specify **trap-name** as required to enable the trap function for one or more events.

NOTE

The device has the trap suppression function configured and does not report traps within 10 minutes.

Example

Enable all traps of the AM module.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name mid_am
```

Related Topics

8.3.74 display snmp-agent trap feature-name mid_am all

8.3.108 static-bind

Function

The **static-bind** command binds an IP address in a global address pool to a MAC address of a client.

The **undo static-bind** command unbinds the IP address in a global address pool from a MAC address.

Copyright © Huawei Technologies Co., Ltd.

By default, the IP address in a global address pool is not bound to any MAC address.

Format

static-bind ip-address *ip-address* **mac-address** *mac-address* [**option-template** *template-name* | **description** *description*]

undo static-bind [**ip-address** *ip-address* | **mac-address** *mac-address*]

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the IP address to be bound. The IP address must be a valid IP address in the global address pool.	The value is in dotted decimal notation.
mac-address *mac-address*	Specifies the user MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
option-template *template-name*	Specifies the name of the DHCP Option template. To allocate network configuration parameters except IP addresses to static clients, specify the parameter. Before specifying the parameter, run the **dhcp option template** command to create a DHCP option template, and configure network parameters for static clients in the DHCP Option template view.	The name is a string of 1 to 31 case-sensitive characters without spaces.
description *description*	Specifies the user description.	The value is a string of 1 to 256 case-sensitive characters. It can contain spaces.

Views

IP address pool view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **static-bind** command applies to DHCP servers. When planning a network, you need to allocate fixed IP addresses to some important hosts to ensure reliability. In this case, you can bind IP addresses in the address pool to the MAC addresses of these hosts. After the preceding configuration is complete, if the host of the MAC address to which the IP address is bound request an IP address from the DHCP server, the DHCP server finds the bound IP address based on the host's MAC address and allocates this IP address to the host, ensuring that the IP address obtained by the host is fixed.

You can run the **static-bind** command to bind an IP address in a global address pool to a MAC address.

You can run the **dhcp server static-bind** command to bind an IP address in an interface address pool to a MAC address.

Prerequisites

Network segment addresses that can be assigned from the global address pool have been configured using the **network (IP address pool view)** command.

Precautions

- Ensure that the bound IP address is not configured as the IP address that cannot be allocated using the **8.3.77 excluded-ip-address** command and is not allocated by the DHCP server.
- You can run the **display ip pool** command to view the used IP addresses in the current address pool and select an available IP address to be bound to the MAC address. To bind used IP addresses to MAC addresses, run the **reset ip pool** command to reclaim used IP addresses first. IP addresses that are used can also be statically bound to MAC addresses or unbound from MAC addresses. When an IP address is statically bound to a MAC address, ensure that the MAC address to be bound is the same as the MAC address of the user who actually uses the IP address.
- The DHCP server preferentially allocates the IP address that has been statically bound to the client's MAC address.
- After an IP address is bound to a MAC address, the IP address does not expire; the binding between the IP and MAC addresses cannot be deleted when the IP address is in use. After an IP address is bound to a MAC address, the IP address does not expire. After an automatically allocated IP address is statically bound to a MAC address, the lease time of the IP address becomes unlimited. After the static binding between the IP address and the MAC address is deleted, the lease time of the IP address becomes the same as that configured in the address pool.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure a DHCP server to assign a fixed IP address 192.168.1.10 in the global address pool **global1** to a host with the MAC address dcd2-fc96-e4c0.

```
<Huawei> system-view
[Huawei] ip pool global1
[Huawei-ip-pool-global1] network 192.168.1.10 mask 24
[Huawei-ip-pool-global1] static-bind ip-address 192.168.1.10 mac-address dcd2-fc96-e4c0
```

Related Topics

8.3.83 ip pool (system view)

8.3.55 dhcp server static-bind

8.3.20 dhcp option template

8.3.109 vpn-instance (DHCP server group view)

Function

The **vpn-instance** command binds a DHCP server group to a VPN instance.

The **undo vpn-instance** command unbinds the VPN instance from a DHCP server group.

By default, no DHCP server is bound to a VPN instance.

Format

vpn-instance *vpn-instance-name*

undo vpn-instance

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance.	The value must be an existing VPN instance on the device.

Views

DHCP server group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Copyright © Huawei Technologies Co., Ltd.

This command applies to DHCP relay agents. To apply DHCP services in a VPN instance, you need to run the **vpn-instance** command to bind the created DHCP server group to the VPN instance.

Prerequisites

A VPN instance has been created using the **ip vpn-instance** command.

Precautions

The VPN instance bound to the DHCP server group on the DHCP relay agent must be the same as the VPN instance bound to the IP address pool on the DHCP server; otherwise, users in the IP address pool cannot go online.

Example

Bind DHCP server group **dhcp-srv1** to VPN instance **huawei**.

```
<Huawei> system-view
[Huawei] ip vpn-instance huawei
[Huawei-vpn-instance-huawei] ipv4-family
[Huawei-vpn-instance-huawei-af-ipv4] route-distinguisher 22:1
[Huawei-vpn-instance-huawei-af-ipv4] quit
[Huawei-vpn-instance-huawei] quit
[Huawei] dhcp server group dhcp-srv1
[Huawei-dhcp-server-group-dhcp-srv1] vpn-instance huawei
```

Related Topics

8.3.40 dhcp server group

8.3.110 vpn-instance (global address pool view)

Function

The **vpn-instance** command binds an IP address pool to a VPN instance.

The **undo vpn-instance** command restores the default setting.

By default, an IP address pool is not bound to any VPN instance.

Format

vpn-instance *vpn-instance-name*

undo vpn-instance

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance.	The value must be an existing VPN instance on the device.

Copyright © Huawei Technologies Co., Ltd.

Views

Global address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. To apply DHCP services in a VPN instance, you need to run the **vpn-instance** command to bind the created IP address pool to the VPN instance.

Prerequisites

A VPN instance has been created using the **ip vpn-instance** command.

Precautions

- The VPN instance bound to the IP address pool on the DHCP server must be the same as the VPN instance bound to the DHCP server group on the DHCP relay agent; otherwise, users in the IP address pool cannot go online using this DHCP server group.
- If an IP address pool is bound to a VPN instance, IP addresses assigned from this address pool are VPN addresses.
- To bind an interface address pool to a VPN instance, run the **ip binding vpn-instance** command in the interface view.

Example

Bind the address pool **global1** to the VPN instance **huawei**.

```
<Huawei> system-view
[Huawei] ip vpn-instance huawei
[Huawei-vpn-instance-huawei] ipv4-family
[Huawei-vpn-instance-huawei-af-ipv4] route-distinguisher 22:1
[Huawei-vpn-instance-huawei-af-ipv4] quit
[Huawei-vpn-instance-huawei] quit
[Huawei] ip pool global1
[Huawei-ip-pool-global1] vpn-instance huawei
```

Related Topics

8.3.83 ip pool (system view)

12.9.33 ip binding vpn-instance

8.4 DNS Configuration Commands

Copyright © Huawei Technologies Co., Ltd.

8.4.1 ddns apply policy

Function

The **ddns apply policy** command allows you to apply DDNS policies on interfaces.

The **undo ddns apply policy** command deletes the configuration.

By default, no DDNS policy is bound to an interface.

Format

ddns apply policy *policy-name* [**fqdn** *domain-name*]

undo ddns apply policy [*policy-name*]

Parameters

Parameter	Description	Value
policy-name	Specifies a DDNS policy name.	The value must be the name of an existing DDNS policy.
fqdn *domain-name*	Specifies domain name updated by the DDNS.	The value is a string of 1 to 128 case-sensitive characters without spaces.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

DNS provides static mappings between domain names and IP addresses. When IP addresses of interfaces change, DNS cannot dynamically update mappings. After the specified DDNS policy is applied on an interface, if the IP address of the interface changes, the DDNS policy updates mapping between the specified Fully Qualified Domain Name (FQDN) and the IP address.

If a DDNS policy with the same name is bound to an interface repeatedly and different FQDNs are specified, only the latest configuration takes effect and a DDNS update is initiated.

Prerequisites

To apply the policy on an interface, you need to create the DDNS policy first, also the DDNS policy, including DDNS Server domain-name, DDNS Client domain-name, username and password, must be completely configured.

Copyright © Huawei Technologies Co., Ltd.

Example

Apply the DDNS policy "test "on the Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] ddns apply policy test
```

Related Topics

8.4.11 ddns policy

8.4.2 display ddns interface

Function

The **display ddns interface** command displays information about the interfaces to which DDNS policies are applied.

Format

display ddns interface { **all** | *interface-type interface-number* }

Parameters

Parameter	Description	Value
all	Indicates all interfaces.	-
interface-type interface-number	Specifies the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view information about the interfaces to which DDNS policies are applied, run the **display ddns interface** command.

Example

Display the configuration of DDNS policies applied to Eth2/0/0.

```
<Huawei> display ddns interface ethernet 2/0/0
 Policies applied on interface Ethernet2/0/0 :
 ------------------------------------------------------------------------------
 Policy name         : 123
 Server              : ns.huawwei.com
 User name           : -
 Password            : -
```


Copyright © Huawei Technologies Co., Ltd.

```
Update method        : ddns
Update interval      : 3600 seconds
Current status       : START
Client FQDN          : 123
Client IP            : 0.0.0.0
Server IP            : -
Last update time     : 2015-10-27 10:30:28
Last update result   : Update failed
```

Table 8-38 Description of the **display ddns interface** command output

Item	Description
Policy name	DDNS policy name.
Server	Domain name of a DDN service provider.
User name	User name used for access to a DDNS service provider.
Password	Password used for access to a DDNS service provider.
Update method	DDNS update method: • **http**: common HTTP update method • **vendor-specific**: vendor-defined update method • **ddns**: update method compliant with RFC 2136, which updates only A records. • **ddns both**: update method compliant with RFC 2136, which updates A and PTR records.
Update interval	Interval at which a DDNS client initiates a DDNS update, in seconds.
Current status	Status of an applied DDNS policy: • INIT: Initial state. • ESTABLISH: Update is successful. • AUTHENTICATION FAILED: Authentication failed. • START: Update starts.
Client FQDN	Domain name of a DDNS client.
Client IP	IP address of a DDNS client.
Server IP	IP address of a DDNS server.
Last update time	Last update time.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Last update result	Last update result: • Success: The update is successful. • Resolve ddns server domain name fail: Failed to parse the domain name of the DDNS server. • Authentication fail: Authentication failed. • Update failed: The update failed. • Updating: The update is ongoing.

8.4.3 display ddns policy

Function

The **display ddns policy** command displays DDNS policy information.

Format

display ddns policy [*policy-name*]

Parameters

Parameter	Description	Value
policy-name	Displays information about a specified DDNS policy	The DDNS policy name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ddns policy** command to view DDNS policy information. If no *policy-name* is specified, all DDNS policies information is displayed.

Example

Display current DDNS policy information.

```
<Huawei> display ddns policy test
 Policy name          : test
```

 Copyright © Huawei Technologies Co., Ltd.

```
Server              : oray://username:password@phddnsdev.oray.net
User name           : -
Password            : -
Update method       : vendor-specific
Update interval     : 3600 seconds
Apply interface     : Ethernet2/0/0
```

Table 8-39 Description of the **display ddns policy** command output

Item	Description
Policy name	DDNS policy name.
Server	Domain-name of a DDNS service provider
User name	User name for accessing a DDNS service provider
Password	Password for accessing a DDNS service provider
Update method	Update mode of the DDNS Client. • **http**: indicates the update mode of common http. • **vendor-specific**: indicates the update mode defined by the vendors. • **ddns**: indicates the update mode defined by RFC2136, which only updates Class-A records. • **ddns both**: indicates the update mode defined by RFC2136, which updates Class-A records and PTR records.
Update interval	Interval for which the DDNS client initiates DDNS updates, in second.
Apply interface	Interface that applies this policy

8.4.4 display dns configuration

Function

The **display dns configuration** command displays the global DNS configurations.

Format

display dns configuration

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the global DNS configurations.

```
<Huawei> display dns configuration
------------------------------------------------------------------------------
Dns resolve                    : Disabled
DNS-server-select-algorithm    : Auto
Dns server source ip address   : -
Dns server source ipv6 address : -
Dns proxy                      : Disabled
Dns IPv6 proxy                 : Disabled
Dns relay                      : Disabled
Dns IPv6 relay                 : Disabled
Dns spoofing                   : -
Dns IPv6 spoofing              : -
Dns forward retry-number       : 2
Dns forward retry-timeout      : 3
Dns server vpn-instance        : vpn1
------------------------------------------------------------------------------
```

Table 8-40 Description of the **display dns configuration** command output

Item	Description
Dns resolve	Whether dynamic DNS resolution is enabled. The value can be: • Enabled: Dynamic DNS resolution is enabled. • Disabled: Dynamic DNS resolution is disabled. To enable dynamic DNS resolution, run the **dns resolve** command.
DNS-server-select-algorithm	Algorithm for selecting a destination DNS server. The value can be: • Fixed: The destination DNS server is selected in fixed order. • Auto: The destination DNS server is selected in auto order. To specify an algorithm for selecting a destination DNS server, run the **dns-server-select-algorithm** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Dns server source ip address	Source IP address of the local device for communication. To set the source IP address of the local device, run the **dns server source-ip** command.
Dns server source ipv6 address	Source IPv6 address of the local device for communication. To set the source IPv6 address of the local device, run the **dns server ipv6 source-ip** command.
Dns proxy	Whether DNS proxy is enabled. The value can be: • Enabled: DNS proxy is enabled. • Disabled: DNS proxy is disabled. To enable DNS proxy, run the **dns proxy enable** command.
Dns IPv6 proxy	Whether IPv6 DNS proxy is enabled. The value can be: • Enabled: IPv6 DNS proxy is enabled. • Disabled: IPv6 DNS proxy is disabled. To enable DNS proxy, run the **dns proxy ipv6 enable** command.
Dns relay	Whether DNS relay is enabled. The value can be: • Enabled: DNS relay is enabled. • Disabled: DNS relay is disabled. To enable DNS relay, run the **dns relay enable** command.
Dns IPv6 relay	Whether IPv6 DNS relay is enabled. The value can be: • Enabled: IPv6 DNS relay is enabled. • Disabled: IPv6 DNS relay is disabled. To enable IPv6 DNS relay, run the **dns relay ipv6 enable** command.
Dns spoofing	IP address that spoofs Reply packets. To enable DNS spoofing and specify the IP address that spoofs Reply packets, run the **dns spoofing** command.
Dns IPv6 spoofing	IPv6 address that spoofs Reply packets. To enable DNS spoofing and specify the IPv6 address that spoofs Reply packets, run the **dns spoofing ipv6** command.
Dns forward retry-number	Number of times for retransmitting query messages to the destination DNS server. To set the number of times for retransmitting query messages to the destination DNS server, run the **dns forward retry-number** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Dns forward retry-timeout	Retransmission timeout period that the device sends query messages to the destination DNS server. To set the retransmission timeout period that the device sends query messages to the destination DNS server, run the **dns forward retry-timeout** command.
Dns server vpn-instance	Name of the VPN instance that the DNS server belongs to. If the VPN instance that the DNS server belongs to is not specified, this parameter is not displayed. To configure the name of the VPN instance that the DNS server belongs to, run the **dns server vpn-instance** command.

8.4.5 display dns domain

Function

The **display dns domain** command displays the configuration and sequence of domain name suffixes.

Format

display dns domain [**verbose**]

Parameters

Parameter	Description	Value
verbose	Displays the detail information of domain name suffixes.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display dns domain** command to view the configuration and sequence of domain name suffixes.

Example

Display the list of domain name suffixes.

```
<Huawei> display dns domain
Type:
```


Copyright © Huawei Technologies Co., Ltd.

```
D:Dynamic    S:Static

NO.  Type    Domain name                    TTL
1    S       com                            -
2    S       net                            -
```

Table 8-41 Description of the **display dns domain** command output

Item	Description
NO.	Domain name suffix numbers, that is, the configuration sequence of domain name suffixes.
Type	Domain name suffixes type, including dynamic and static domain name suffix.
Domain name	Configured domain name suffix. In this example, two domain name suffixes are displayed. During DNS resolution, the first suffix "com" is added and sent to the DNS server. If the DNS server gives no response, the query message is resent. If the DNS server still gives no response, the query message is resent for a third time. If the DNS server still does not respond, the second suffix "net" is added and sent to the DNS server for searching for the mapped address.
TTL	Domain name suffix TTL.

Related Topics

8.4.12 dns domain

8.4.6 display dns dynamic-host

Function

The **display dns dynamic-host** command displays dynamic DNS entries saved in the domain name cache.

Format

display dns dynamic-host [**ip** | **naptr** | **srv**] [*domain-name*]

Parameters

Parameter	Description	Value
ip	Specifies the Class-A and PTR query dynamic DNS entries.	-
naptr	Specifies the NAPTR query dynamic DNS entries.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
srv	Specifies the SRV query dynamic DNS entries.	-
domain-name	Specifies the dynamic DNS entries of a domain name.	The value must be an existing domain name suffix.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display dns dynamic-host** command to view dynamic DNS entries saved in the domain name cache and check whether domain names match the mapping entries.

Example

Display the dynamic DNS entries saved in the domain name cache.

```
<Huawei> display dns dynamic-host
Host                          TTL       Type   Address
sipx.autosrv.com               114       IP     192.168.1.1
sip.autosrv.com                237       IP     192.168.1.2
sip.autonaptr.com              117       IP     192.168.1.3
_sip._tcp.autosrv.com           55       SRV    0 0 0 sipx.autosrv.com
                                         0 0 0 sip.autosrv.com
autonaptr.com                   0         NAPTR  101 10 A SIP+D2T  sip.autona

Total  :  5
```

Table 8-42 Description of the **display dns dynamic-host** command output

Item	Description
Host	Domain name. • sipx.autosrv.com: indicates the domain name of the server providing the SIP service. • _sip._tcp.autosrv.com: indicates the domain name of the server providing the SIP service through TCP in autosrv.com. • autonaptr.com: indicates the domain name in the NAPTR resource record.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
TTL	Time left before dynamic DNS entries saved in the cache age out, in seconds.
Type	Query type: • IP: Class-A query, which is used to request the IP address corresponding to a domain name, or Pointer (PTR) query, which is used to request the domain name corresponding to an IP address. • SRV: Service Record (SRV) query, which is used to obtain information about a server based on the protocol running on the server, including the domain name and port number. • NAPTR: Naming Authority Pointer (NAPTR) query, which is used to obtain information about a server based on the server's domain name, including the IP address, and the transmission protocol.
Address	IP address mapping the domain name. • 192.168.1.1: indicates the IPv4 address. • 0 0 0 sipx.autosrv.com: indicates the SRV query result. In the SRV query result, **0 0 0** indicates the priority, weight, and port number respectively, and **sipx.autosrv.com** indicates the domain name of the server providing the SIP service. • 101 10 A SIP+D2T sip.autona: indicates the NAPTR query result. In the NAPTR query result, **101 10** indicates the NAPTR resource record sequence and priority; **A** indicates that the IP address to be queried; **SIP+D2T** indicates that SIP and TCP are used; **sip.autona** indicates the domain name to be queried.

Related Topics

8.4.29 reset dns dynamic-host

Copyright © Huawei Technologies Co., Ltd.

8.4.7 display dns forward table

Function

The **display dns forward table** command displays the DNS forwarding table, including the mapping entry of the source IP address in a specified DNS query message.

Format

display dns forward table [**source-ip** *ip-address*]

Parameters

Parameter	Description	Value
source-ip *ip-address*	Specifies the source IP address in query messages.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After DNS proxy or DNS relay is enabled, you can run the **display dns forward table** command to view the DNS table of IP addresses.

NOTE

When the device receives DNS request packets from the client but does not receive DNS reply packets from the server, you need to run the **display dns forward table** command to view the DNS forwarding table.

Example

Display the DNS table on the DNS proxy or DNS relay.

```
<Huawei> display dns forward table
Domain name            : www.domain.com
Source IP              : 10.136.128.53
Source port            : 2055
Source packet id       : 3562
Forward packet id      : 60669
Query type             : 1
VPN-Instance           : vpna
```

 Copyright © Huawei Technologies Co., Ltd.

Table 8-43 Description of the display dns forward table command output

Item	Description
Domain name	Domain name.
Source IP	IP address of the client.
Source port	Port number of the client.
Source packet id	ID of the request packet from the client.
Forward packet id	ID of the forwarded packet, which corresponds to the ID of the request packet from the client.
Query type	Query type: • 1: Class-A query • 12: Pointer Record (PTR) query • 33: SRV query • 35: NAPTR query
VPN-Instance	Name of the VPN instance that the DNS client belongs to.

8.4.8 display dns statistics

Function

The **display dns statistics** command displays statistics on DNS packets.

Format

display dns statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check statistics on DNS packets, including the DNS IPv4 and IPv6 addresses.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display statistics on DNS packets.

```
<Huawei> display dns statistics

SumFromDNSv4Client          : 0
SumToDNSv4Client            : 0
SumFromDNSv4Server          : 0
SumToDNSv4Server            : 0

SumFromDNSv6Client          : 0
SumToDNSv6Client            : 0
SumFromDNSv6Server          : 0
SumToDNSv6Server            : 0

RetryFromClient             : 0
NotQueryFromClient          : 0
ParseFailFromClient         : 0
TooLongFromClient           : 0
LocalQueryFromClient        : 0
NotStandardQueryFromClient  : 0

NotRespFromServer           : 0
NoAnswerFromServer          : 0
ParseFailFromServer         : 0
TooLongFromServer           : 0
ErrorRespFromServer         : 0
NotStandardQueryFromServer  : 0

ResolvePolicyRuleDeny       : 0
```

Table 8-44 Description of the **display dns statistics** command output

Item	Description
SumFromDNSv4Client	Total number of packets sent from IPv4 DNS clients.
SumToDNSv4Client	Total number of packets sent to IPv4 DNS clients.
SumFromDNSv4Server	Total number of packets sent from IPv4 DNS servers.
SumToDNSv4Server	Total number of packets sent to IPv4 DNS servers.
SumFromDNSv6Client	Total number of packets sent from IPv6 DNS clients.
SumToDNSv6Client	Total number of packets sent to IPv6 DNS clients.
SumFromDNSv6Server	Total number of packets sent from IPv6 DNS servers.
SumToDNSv6Server	Total number of packets sent to IPv6 DNS servers.
RetryFromClient	Number of packets retransmitted from clients.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
NotQueryFromClient	Number of non-query packets sent from clients.
ParseFailFromClient	Number of packets that failed to be parsed and are sent from clients.
TooLongFromClient	Number of packets longer than 512 bytes sent from clients.
LocalQueryFromClient	Number of query packets of which the source address is a local address and sent from clients.
NotStandardQueryFromClient	Number of nonstandard query packets sent from clients.
NotRespFromServer	Number of non-response packets sent from servers.
NoAnswerFromServer	Number of response packets of which the ANCOUNT field is 0 and sent from servers.
ParseFailFromServer	Number of packets that failed to be parsed and are sent from servers.
TooLongFromServer	Number of packets longer than 512 bytes sent from servers.
ErrorRespFromServer	Number of error response packets sent from servers.
NotStandardQueryFromServer	Number of nonstandard query packets sent from servers.
ResolvePolicyRuleDeny	Times of resolve policy rule deny.

8.4.9 display dns server

Function

The **display dns server** command displays the configuration and sequence of the current DNS server.

Format

display dns server [**verbose**]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
verbose	Displays detailed information about the DNS server.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring DNS, run the **display dns server** command to view the configuration and sequence of current DNS servers.

Example

Display configurations of a DNS server.

```
<Huawei> display dns server
Type:
D:Dynamic     S:Static

IPv4 DNS server :
NO. Type Status Used IP Address
0   S    -      Yes  10.1.1.1
1   S    -      Yes  10.1.1.2
2   D    Up     Yes  10.1.1.2
3   D    Up     Yes  10.1.1.3

IPv6 DNS servers :
NO. Type Status Used IPv6 Address                    Interface
0   S    -      Yes  FC00:1::1                      -
1   D    -      Yes  FC00:1::1                      -
2   D    -      Yes  FC00:1::2                      -
```

Table 8-45 Description of the **display dns server** command output

Item	Description
Type	Configuration type of the DNS server IP address, including dynamic and static.
IPv4 DNS server	IPv4 DNS server configuration.
NO.	DNS server number, indicating the order in which they were configured.
Status	DNS server status.
Used	Indicates whether the DNS server is used.
IP Address	IPv4 address of the DNS server.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
IPv6 Address	IPv6 address of the DNS server.
IPv6 DNS servers	IPv6 DNS server configuration.
Interface	Name of the outbound interface communicating with the DNS server.

Related Topics

8.4.19 dns server

8.4.10 display ip host

Function

The **display ip host** command displays mappings between hosts and IP addresses.

Format

display ip host

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring static DNS entries, you can run the **display ip host** command to view the mapping between hosts and IP addresses.

Example

Display mappings between hosts and IP addresses.

```
<Huawei> display ip host
Host                  Age        Flags  Address
example                 0       static 10.2.2.2
```


Copyright © Huawei Technologies Co., Ltd.

Table 8-46 Description of the **display ip host** output of the command

Item	Description
Host	Host name.
Age	Aging time. The value 0 indicates that the static DNS entry need not be aged.
Flags	Status of the domain name. "Static" indicates the static domain name.
Address	IP address matching the host.

8.4.11 ddns policy

Function

The **ddns policy** command creates a DDNS policy and enters the DDNS policy view.

The **undo ddns policy** command deletes a DDNS policy.

By default, no DDNS policy is created in the system.

Format

ddns policy *policy-name*

undo ddns policy *policy-name*

Parameters

Parameter	Description	Value
policy-name	Specifies the name of the DDNS policy.	The value is a string of 1 to 32 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

DNS provides static mappings between domain names and IP addresses. When IP addresses of nodes change, DNS cannot dynamically update mappings. If a DNS

 Copyright © Huawei Technologies Co., Ltd.

client uses the original domain name to access the node, the DNS client will fail to access the node because the IP address mapping the domain name is incorrect. The DDNS updates the mappings between the domain name and the IP address on the DNS server to ensure that the IP address can be resolved correctly. The device can function as a DDNS client. When the IP address of the interface that provides services changes, the device sends a request of updating the domain name entry to the DDNS server. After receiving the request, the DDNS server updates the domain name entry.

Example

Create a DDNS policy "test ".

```
<Huawei> system-view
[Huawei] ddns policy test
[Huawei-ddns-policy-test]
```

8.4.12 dns domain

Function

The **dns domain** command configures a domain name suffix of a server or a host on a DNS client that the DNS client wants to access.

The **undo dns domain** command deletes a configured domain name suffix from a DNS client.

By default, no domain name suffix is configured on a DNS client.

Format

dns domain *domain-name*

undo dns domain [*domain-name*]

Parameters

Parameter	Description	Value
domain-name	Specifies a domain name suffix on a DNS Client.	The value is a string of 1 to 64 characters, spaces not supported. The string is a combination of digits, letters, underscores (_), dots (.), and hyphen (-).

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Application Scenario

 Copyright © Huawei Technologies Co., Ltd.

Generally, the domain name suffixes of some servers or hosts that a DNS client accesses are the same, for example, com.cn. In this case, you can set the domain name suffixes. When a DNS client accesses a host:

- If the entered domain name does not carry dots (.), for example, "huawei", the system first adds the suffix com.cn to the domain name and sends a domain name request of "huawei.com.cn" to the DNS server to find the IP address corresponding to the domain name. If the DNS client does not receive any response from the server, it sends a domain name request of "huawei" to the DNS server to find the IP address corresponding to the domain name.
- If the entered domain name carries dots (.), for example, "ilite.huawei", the system first sends a domain name request of "ilite.huawei" to the DNS server to find the IP address corresponding to the domain name. If the DNS client does not receive any response from the server, it adds the suffix com.cn to the domain name and sends a domain name request of "ilite.huawei.com.cn" to the DNS server to find the IP address corresponding to the domain name.

Precautions

A DNS client supports a maximum of 10 domain name suffixes. To configure multiple domain name suffixes, you can run the **dns domain** command repeatedly.

If the name of the suffix to be deleted is specified, the specified suffix is deleted. Otherwise, all the suffixes are deleted.

Example

Configure a domain name suffix as com.cn.

```
<Huawei> system-view
[Huawei] dns domain com.cn
```

Related Topics

8.4.5 display dns domain

8.4.13 dns forward retry-number

Function

The **dns forward retry-number** command sets the number of times for the device to retransmit query requests to the destination DNS server.

The **undo dns forward retry-number** command restores the default retransmission count.

By default, the retransmission count is 2.

Format

dns forward retry-number *number*

undo dns forward retry-number

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
number	Specifies the number of times for the device to retransmit query requests to the destination DNS server.	The value is an integer from 0 to 15.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The mode for a device to select the destination DNS server can be **auto** and **fixed**. For how a device sends DNS request packets to the destination DNS server in each mode and the corresponding precautions, see **8.4.22 dns-server-select-algorithm**.

If the number of times for the device to retransmit DNS request packets to each destination DNS server is relatively large and the packet retransmission timeout period is relatively long, the time for the DNS client to wait for the response from the DNS server is too long. However, the request timeout period of the DNS client is shorter, so that the DNS client fails to properly receive response packets from the server. To enable the DNS server to rapidly respond DNS request packets, you can run the **dns forward retry-number** and **dns forward retry-timeout** commands to adjust the number of times for the device to retransmit DNS request packets to each DNS server and the packet retransmission timeout period for ensuring that the DNS client can properly receive response packets from the server.

You need to consider the number of times for the device to retransmit DNS query requests to the destination DNS server, retransmission timeout period, and mode for the device to select the DNS server into consideration before configuring the query timeout period on a device.

- When the mode for a device to select the destination DNS server is **auto**, the query timeout period of a DNS device is calculated as follows: (Number of retransmission times + 1) x Retransmission timeout period
- When the mode for a device to select the destination DNS server is **fixed**, the query timeout period of a DNS device is calculated as follows: (Number of retransmission times + 1) x Retransmission timeout period x Number of DNS servers

Example

Set the retransmission count that the device sends query packets to the destination DNS server to 1.

Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] dns forward retry-number 1
```

8.4.14 dns forward retry-timeout

Function

The **dns forward retry-timeout** command sets the retransmission timeout period that the device sends Query packets to the destination DNS server.

The **undo dns forward retry-timeout** command restores the default retransmission timeout period.

By default, the retransmission timeout period for which the device sends DNS query requests to the destination DNS server is 3 seconds.

Format

dns forward retry-timeout *time*

undo dns forward retry-timeout

Parameters

Parameter	Description	Value
time	Specifies the retransmission timeout period that the device sends Query packets to the destination DNS server.	The value is an integer that ranges from 1 to 15, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The mode for a device to select the destination DNS server can be **auto** and **fixed**. For how a device sends DNS request packets to the destination DNS server in each mode and the corresponding precautions, see **8.4.22 dns-server-select-algorithm**.

If the number of times for the device to retransmit DNS request packets to each destination DNS server is relatively large and the packet retransmission timeout period is relatively long, the time for the DNS client to wait for the response from the DNS server is too long. However, the request timeout period of the DNS client is shorter, so that the DNS client fails to properly receive response packets from the server. To enable the DNS server to rapidly respond DNS request packets, you

Copyright © Huawei Technologies Co., Ltd.

can run the **dns forward retry-number** and **dns forward retry-timeout** commands to adjust the number of times for the device to retransmit DNS request packets to each DNS server and the packet retransmission timeout period for ensuring that the DNS client can properly receive response packets from the server.

You need to consider the number of times for the device to retransmit DNS query requests to the destination DNS server, retransmission timeout period, and mode for the device to select the DNS server into consideration before configuring the query timeout period on a device.

- When the mode for a device to select the destination DNS server is **auto**, the query timeout period of a DNS device is calculated as follows: (Number of retransmission times + 1) x Retransmission timeout period
- When the mode for a device to select the destination DNS server is **fixed**, the query timeout period of a DNS device is calculated as follows: (Number of retransmission times + 1) x Retransmission timeout period x Number of DNS servers

Example

Set the retransmission timeout period that the device sends Query packets to the destination DNS server to 2 seconds.

```
<Huawei> system-view
[Huawei] dns forward retry-timeout 2
```

8.4.15 dns proxy enable

Function

The **dns proxy enable** command enables DNS proxy.

The **undo dns proxy enable** command disables DNS proxy.

By default, DNS proxy is disabled.

Format

dns proxy enable

undo dns proxy enable

Parameters

None

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

DNS proxy is used to forward DNS requests and reply packets between the DNS client and DNS server. The DNS client sends a DNS request packet to the device on which DNS proxy is enabled. The device sends the request packet to the DNS server and sends the reply packet to the DNS client. The device functions as the DNS proxy to provide services of the DNS server. Users do not need to interact with the DNS server directly. This function simplifies route deployment and improves performance and security of the DNS server.

Example

Enable DNS proxy.

```
<Huawei> system-view
[Huawei] dns proxy enable
```

Disable DNS proxy.

```
<Huawei> system-view
[Huawei] undo dns proxy enable
```

Related Topics

8.4.17 dns relay enable
8.4.7 display dns forward table
8.4.30 reset dns forward table

8.4.16 dns proxy sip-info insert-mode decompression-domain-name

Function

The **dns proxy sip-info insert-mode decompression-domain-name** command inserts SIP server information to DNS response packets in domain name decompression mode when the device functions as a DNS proxy.

The **undo dns proxy sip-info insert-mode decompression-domain-name** command restores the default insert mode.

By default, the domain name decompression mode is not used.

Format

dns proxy sip-info insert-mode decompression-domain-name

undo dns proxy sip-info insert-mode decompression-domain-name

Parameters

None

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

This command applies only to the Branch Exchange Survivable Telephony (BEST) solution. In the BEST solution, the phone functions as the DNS client and the device functions as the DNS proxy. When the DNS client initiates an SRV query, the device inserts SIP server information to the DNS response packet. For example, when a Cisco phone is used and the **dns proxy sip-info insert-mode decompression-domain-name** command is not used to insert SIP server information to DNS response packets in domain name decompression mode, the phone cannot resolve DNS response packets that have SIP server information inserted.

Example

Insert SIP server information to DNS response packets in domain name decompression mode in the BEST solution.

```
<Huawei> system-view
[Huawei] dns resolve
[Huawei] dns proxy enable
[Huawei] dns proxy sip-info insert-mode decompression-domain-name
```

8.4.17 dns relay enable

Function

The **dns relay enable** command enables DNS relay.

The **undo dns relay enable** command disables DNS relay.

By default, DNS relay is disabled.

Format

dns relay enable

undo dns relay enable

Parameters

None

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

DNS relay is used to forward DNS requests and reply packets between the DNS client and DNS server. The DNS client sends a DNS request packet to the device on which DNS relay is enabled. The device sends the request packet to the DNS server and sends the reply packet to the DNS client. The device functions as the DNS relay to provide services of the DNS server. Users do not need to interact with the DNS server directly. This function simplifies route deployment and improves performance and security of the DNS server.

Example

Enable DNS relay.

```
<Huawei> system-view
[Huawei] dns relay enable
```

Disable DNS relay.

```
<Huawei> system-view
[Huawei] undo dns relay enable
```

Related Topics

8.4.15 dns proxy enable

8.4.7 display dns forward table

8.4.30 reset dns forward table

8.4.18 dns resolve

Function

The **dns resolve** command enables dynamic DNS resolution.

The **undo dns resolve** command disables dynamic DNS resolution.

By default, the dynamic DNS resolution is disabled.

Format

dns resolve

undo dns resolve

Parameters

None

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

To obtain IP addresses mapping domain names using the DNS server, run the **dns resolve** command to enable dynamic DNS resolution on the device.

Example

Enable dynamic DNS resolution.

```
<Huawei> system-view
[Huawei] dns resolve
```

Related Topics

8.4.19 dns server

8.4.19 dns server

Function

The **dns server** command configures an IP address for a DNS server.

The **undo dns server** command deletes the DNS server IP address.

By default, no DNS server IP address is configured.

Format

dns server *ip-address* [**track nqa** *admin-name test-name*]

undo dns server [*ip-address*]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a DNS server.	The value is in dotted decimal notation.
track nqa *admin-name test-name*	Specifies the NQA test instance to be associated with the DNS server. • *admin-name*: specifies the name of the administrator for the NQA test instance. • *test-name*: specifies the name of the NQA test instance.	The value is a string of 1 to 32 case-sensitive characters without any space.

Views

System view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A maximum of six DNS servers can be specified on Router. During dynamic DNS resolution, query messages are sent to DNS servers based on the configuration sequence of DNS servers.

The system sends a query to the DNS server first configured. If no response is received in the specified period of time (which can be configured by running the command **8.4.14 dns forward retry-timeout**), it resends the query twice. If receiving no response for the specified times (which can be configured by running the command **8.4.13 dns forward retry-number**), the system sends the query to the DNS server second configured and so on.

Prerequisites

Before specifying the NQA test instance to be associated with the DNS server using **track nqa** *admin-name test-name*, perform the following operations and start the NQA test instance.

- Configuring and starting an NQA test instance of the DNS type
  a. Run the **system-view** command to enter the system view.
  b. Run the **nqa test-instance** *admin-name test-name* command to create an NQA test instance and enter the test instance view.
  c. Run the **test-type dns** command to configure the test type to DNS.
  d. Run the **dns-server ipv4** *ip-address* command to configure the DNS server address.
  e. Run the **destination-address url** *urlstring* command to configure the destination host name.
  f. Run the **frequency** *interval* command to set the automatic test interval for the NQA test instance.
  g. Run the **start** command to start the NQA test instance.

     An NQA test instance can be started immediately, at a specified time, or after a specified delay.

     - Run the **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }] command to start the test instance immediately.
     - Run the **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }] command to start the test instance at a specified time.
     - Run the **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }] command to start the test instance after a specified delay.

 Copyright © Huawei Technologies Co., Ltd.

- Configuring and starting an NQA test instance of the ICMP type
  a. Run the **system-view** command to enter the system view.
  b. Run the **nqa test-instance** *admin-name test-name* command to create an NQA test instance and enter the test instance view.
  c. Run the **test-type icmp** command to configure the test type to ICMP.
  d. Run the **destination-address ipv4** *ipv4-address* command to configure the destination IP address.
  e. Run the **frequency** *interval* command to set the automatic test interval for the NQA test instance.
  f. Run the **start** command to start the NQA test instance.

     An NQA test instance can be started immediately, at a specified time, or after a specified delay.

     - Run the **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }] command to start the test instance immediately.
     - Run the **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }] command to start the test instance at a specified time.
     - Run the **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }] command to start the test instance after a specified delay.

Example

Assign the IP address 10.2.0.70 to the DNS server.

```
<Huawei> system-view
[Huawei] dns server 10.2.0.70
```

Related Topics

8.4.9 display dns server

8.4.20 dns server vpn-instance

Function

The **dns server vpn-instance** command configures the device to send DNS query requests to the DNS server on a specified VPN network.

The **undo dns server vpn-instance** command disables the device from sending DNS query requests to the DNS server on a specified VPN network.

By default, the device can only send DNS query requests to the DNS server on a public network.

Format

dns server vpn-instance *vpn-instance-name*

Copyright © Huawei Technologies Co., Ltd.

undo dns server vpn-instance

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies a VPN instance name.	It must be the name of an existing VPN instance.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If an interface on the device and the DNS server have reachable routes to each other and the interface is on a VPN network, the device must use the DNS server on the VPN network for DNS query so that DNS packets can be exchanged properly.

NOTE

If you run this command multiple times, only the latest configuration takes effect.

The device can send DNS query requests to the DNS server on a public network or specified VPN network.

The device can respond to DNS query requests sent by DNS clients on multiple VPN networks.

Example

Configure the device to send DNS query requests to the DNS server on the VPN network **vpn1**.

```
<Huawei> system-view
[Huawei] ip vpn-instance vpn1
[Huawei-vpn-instance-vpn1] ipv4-family
[Huawei-vpn-instance-vpn1-af-ipv4] quit
[Huawei-vpn-instance-vpn1] quit
[Huawei] dns server vpn-instance vpn1
```

8.4.21 dns server source-ip

Function

The **dns server source-ip** command configures the source IP address for the device to send and receive DNS packets.

The **undo dns server source-ip** command deletes the source IP address for the device to send and receive DNS packets.

By default, no source IP address is configured for the device.

 Copyright © Huawei Technologies Co., Ltd.

Format

dns server source-ip *ip-address*

undo dns server source-ip

Parameters

Parameter	Description	Value
ip-address	Specifies the source IP address for the device to send and receive DNS packets.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device sends and receives DNS packets, the administrator can specify a source IP address for the device to ensure the communication security. The route from the DNS server to the specified source IP address must be reachable. The DNS server uses the specified source IP address as the destination address and sends a DNS response packet to the local device.

When the device functions as a DNS proxy or relay, run the **dns server source-ip** *ip-address* command to configure the source IP address for communicating with the DNS server.

Precautions

To make the command take effect, pay attention to the following points:

- Ensure that the source IP address is the IP address of an interface or logical interface on the device, and there are reachable routes between the interface and the DNS server.
- Ensure that the source IP address and the IP address of the DNS server are on the same VPN or public network.

Example

Specify source IP address 172.16.1.1 for the local device.

```
<Huawei> system-view
[Huawei] dns server source-ip 172.16.1.1
```

 Copyright © Huawei Technologies Co., Ltd.

8.4.22 dns-server-select-algorithm

Function

The **dns-server-select-algorithm** command configures the DNS server selection mode of the device.

The **undo dns-server-select-algorithm** command restores the default setting.

By default, the device selects a DNS server in **auto** mode.

Format

dns-server-select-algorithm { **fixed** | **auto** }

undo dns-server-select-algorithm

Parameters

Parameter	Description	Value
fixed	Selects a DNS server in **fixed** mode.	-
auto	Selects a DNS server in **auto** mode.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The device can select a DNS server in either of the following modes:

- **auto**: The device uses the internal algorithm to calculate the priorities of all configured DNS servers (IP addresses of DNS servers can be configured by running the **8.4.19 dns server** command), and then sends a DNS query request to the DNS server with the highest priority. If no response is received within a specified period of time, the device retransmits the DNS query request. If the device still does not receive a response from the DNS server after sending query requests multiple times, the device sends the DNS query request to the next server in sequence until it receives a response or has sent to all of the configured DNS servers.
- **fixed**: The device sends a DNS query request to the first DNS server. If no response is received within a specified period of time, the device retransmits the DNS query request. If the device still does not receive a response from the DNS server after sending query requests multiple times, the device sends the

 Copyright © Huawei Technologies Co., Ltd.

DNS query request to the next server in sequence until it receives a response or has sent to all of the configured DNS servers.

NOTE

This function is supported when the device functions as a DNS client or DNS proxy/relay.

When the device functions as a DNS client:

- This function is supported only for DNS query requests sent by IPSec, voice, PKI, or DDNS services.
- The DNS server selection mode is not supported for DNS query requests sent by other services. The device sends the requests according to the order in which DNS servers are configured. If no response is received, the device retransmits the requests according to the order in which DNS servers are configured.

Example

Configure the device to select a DNS server in **fixed** mode.

```
<Huawei> system-view
[Huawei] dns-server-select-algorithm fixed
```

Related Topics

8.4.19 dns server

8.4.23 dns spoofing

Function

The **dns spoofing** command enables DNS spoofing and specifies an IP address in response messages.

The **undo dns spoofing** command disables DNS spoofing.

By default, DNS spoofing is disabled.

Format

dns spoofing *ip-address*

undo dns spoofing

Parameters

Parameter	Description	Value
ip-address	Specifies an IP address in response messages.	The value is in dotted decimal notation.

Views

System view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

If the DNS server address or route to the DNS server is not configured on the DNS proxy or relay, you can enable DNS spoofing on the device to spoof a response message with the configured IP address. Currently, DNS spoofing takes effect for only Class-A query (IP address query based on domain names).

If you run the **dns spoofing** command multiple times, only the latest configuration takes effect.

Example

Enable DNS spoofing and specify the IP address in response messages as 10.1.1.1.

```
<Huawei> system-view
[Huawei] dns spoofing 10.1.1.1
```

Disable DNS spoofing.

```
<Huawei> system-view
[Huawei] undo dns spoofing
```

Related Topics

8.4.17 dns relay enable

8.4.15 dns proxy enable

8.4.24 interval (DDNS policy view)

Function

The **interval** command sets the interval for sending DDNS update requests after the DDNS update is enabled.

The **undo interval** command restores the default setting.

By default, the interval for sending DDNS update requests is 3600 seconds.

Format

interval *interval-time*

undo interval

Parameters

Parameter	Description	Value
interval-time	Specifies interval for sending DDNS update requests.	The value is an integer that ranges from 60 to 31536000, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Views

DDNS policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the interval for sending DDNS update requests is set in the configured DDNS policy, the device is triggered to send DDNS update requests at the specified intervals. All the mappings between IP addresses and domain names defined in the DDNS policy are updated.

Precautions

- If you run the **interval** command multiple times, only the latest configuration takes effect.
- Regardless of whether the interval is reached, the device sends DDNS update requests immediately as long as the primary IP address of the corresponding interface changes or the link status of the interface changes from Down to Up.
- If the interval is changed, the device is triggered to send a DDNS update request immediately.
- When a device is connected to the DDNS server supporting www.oray.cn, this command does not take effect and the device initiates a DDNS update request at a fixed interval of 60 seconds.

Example

Set the interval for sending DDNS update requests to 3600 seconds.

```
<Huawei> system-view
[Huawei] ddns policy mypolicy
[Huawei-ddns-policy-mypolicy] interval 3600
```

8.4.25 ip host

Function

The **ip host** command configures static DNS entries.

The **undo ip host** command deletes static DNS entries.

By default, no static DNS entries are configured.

Format

ip host *host-name ip-address*

undo ip host *host-name* [*ip-address*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
host-name	Specifies the host name.	The value is a string of 1 to 255 case-sensitive characters without spaces.
ip-address	Specifies the IP address mapping the host name.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A static domain name resolution table is manually set up using the **ip host** command, describing the mappings between host names and IP addresses. In addition, some common host names are added to the table. Then, static host name resolution can be performed according to the static domain name resolution table. When requiring the IP address corresponding to a host name, the client first searches the static host name resolution table for the specified host name and obtains the corresponding IP address. In this manner, the efficiency of host name resolution is improved.

Precautions

The **ip host** command configures a maximum of 50 static DNS entries. Each host name can be mapped to only one IP address. When multiple IP addresses are mapped to a host name, only the latest configuration takes effect.

Example

Configure the IP address 10.110.0.1 for the host test.

```
<Huawei> system-view
[Huawei] ip host test 10.110.0.1
```

Related Topics

8.4.10 display ip host

8.4.26 method (DDNS policy view)

Function

The **method** command sets the update mode for the device functioning as a DDNS client.

Copyright © Huawei Technologies Co., Ltd.

The **undo method** command restores the default update mode for the device functioning as a DDNS client.

By default, the update mode is **vendor-specific** for the device functioning as the DDNS client.

Format

method { **ddns** [**both**] | **http** | **vendor-specific** }

undo method

Parameters

Parameter	Description	Value
ddns [**both**]	Indicates that the update mode is ddns (defined by the RFC2136) for the device functioning as a DDNS client. If **both** is specified, both Class-A and PTR query records are updated. If **both** is not specified, only Class-A query records are updated • Class-A query records: mapping between domain names and IP addresses provided by the DNS server for Class-A query. In Class-A query, an IP address is obtained based on a domain name. • PTR query records: mapping between domain names and IP addresses provided by the DNS server for PTR query. In PTR query, a domain name is obtained using an IP address.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
http	Indicates that the update mode is http for the device functioning as a DDNS client. After this parameter is specified, the DDNS client can communicate with a common DDNS server through HTTP.	-
vendor-specific	Indicates that the update mode is vendor-specific for the device functioning as a DDNS client. After this parameter is specified, the DDNS client can communicate with the DDNS servers provided at www.3322.org, www.dyndns.com, and www.oray.cn.	-

Views

DDNS policy view

Default Level

2: Configuration level

Usage Guidelines

When the device functioning as a DDNS client needs to update the mapping between domain names and IP addresses on the DNS server, the following update modes are supported:

- DDNS update mode (defined by the RFC2136): The DDNS client dynamically updates the mapping between domain names and IP addresses on the DNS server. To configure this mode, specify the **ddns** parameter.
- Update mode implemented through the DDNS server: The DDNS client sends the mapping between domain names and IP addresses to the DDNS server with a specified URL. The DDNS server then informs the DNS server to dynamically update the mapping between domain names and IP addresses. To configure this mode, specify the **http** or **vendor-specific** parameter.
  - To use the Siemens DDNS server or DDNS server provided at www.3322.org, www.dyndns.com, or www.oray.cn, specify the **vendor-specific** parameter.
  - To use an HTTP-based common DDNS server, specify the **http** parameter.

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

Security risks exist if the update mode for the device functioning as a DDNS client is set to **http** or **vendor-specific**. It is recommended that you set the update mode to **ddns**.

Example

Set the update mode of the device functioning as the DDNS client to DDNS, and update Class-A and PTR query records.

```
<Huawei> system-view
[Huawei] ddns policy mypolicy
[Huawei-ddns-policy-mypolicy] method ddns both
```

Restore the default update mode for the device functioning as the DDNS client.

```
<Huawei> system-view
[Huawei] ddns policy mypolicy
[Huawei-ddns-policy-mypolicy] undo method
```

Related Topics

8.4.11 ddns policy

8.4.27 name-server (DDNS policy view)

Function

The **name-server** command configures a DNS server to receive update messages from a DDNS client when the device functions as the DDNS client and the update mode is DDNS.

The **undo name-server** command cancels the DNS server configured for receiving update messages from the DDNS client.

By default, no DNS server is configured to receive update messages from a DDNS client when the device functions as the DDNS client and the update mode is DDNS.

Format

name-server *name-server* [**vpn-instance** *vpn-instance-name*]

undo name-server

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
name-server	Specifies the DNS server for receiving update messages from the DDNS client.	The value is a string of 1 to 128 case-sensitive characters without spaces. The value can be a domain name or an IP address.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 characters. The value must be the name of an existing VPN instance.

Views

DDNS policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device functions as a DDNS client and the update mode is DDNS, you can run the **name-server** command to configure a DNS server to receive update messages from the DDNS client. After receiving the update request packets, the DNS server updates the mapping between the domain name and IP address of the DDNS client. When deploying a DNS server on a private network, you need to specify the name of the VPN instance to which the DNS server belongs.

Prerequisites

The update mode of the device functioning as a DDNS client has been set to DDNS using the **8.4.26 method (DDNS policy view)** command.

Example

Configure the DNS server with the domain name **ns.huawei.com** to receive update messages from a DDNS client when the device functions as the DDNS client and the update mode is DDNS.

```
<Huawei> system-view
[Huawei] ddns policy mypolicy
[Huawei-ddns-policy-mypolicy] method ddns
[Huawei-ddns-policy-mypolicy] name-server ns.huawei.com
```

Related Topics

8.4.11 ddns policy

Copyright © Huawei Technologies Co., Ltd.

8.4.28 reset ddns policy

Function

The **reset ddns policy** command configures the device to update mappings between IP addresses and domain names.

Format

reset ddns policy *policy-name* [**interface** *interface-type interface-num*]

Parameters

Parameter	Description	Value
policy *policy-name*	Specifies the name of a DDNS policy that is to be updated.	The value is a string of 1 to 32 case-sensitive characters without spaces.
interface-type interface-num	Specifies the type and number of the interface to which DDNS policies are bound.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

After the **reset ddns policy** command is executed, all mappings between IP addresses and domain names defined in the DDNS policy are updated.

Example

Update the DDNS policy named **dyndns** on GE1/0/0.

```
<Huawei> reset ddns policy dyndns interface gigabitethernet 1/0/0
```

8.4.29 reset dns dynamic-host

Function

The **reset dns dynamic-host** command deletes dynamic DNS entries saved in the domain name cache.

Copyright © Huawei Technologies Co., Ltd.

Format

reset dns dynamic-host

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

NOTICE

Clear dynamic DNS entries with caution because they cannot be restored after being cleared.

After confirming the action of clearing DNS entries, you can run the **reset** command to clear them.

Example

Clear dynamic DNS entries from the domain name cache.

```
<Huawei> reset dns dynamic-host
```

Related Topics

8.4.6 display dns dynamic-host

8.4.30 reset dns forward table

Function

The **reset dns forward table** command clears the DNS entries forwarded.

Format

reset dns forward table [**source-ip** *ip-address*]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
source-ip *ip-address*	Clear the DNS entries of a specified source IP address.	The value is in dotted decimal notation.

Views

User view

Default Level

3: Management level

Usage Guidelines

When the Router as a DNS proxy or relay is attacked, the DNS table will be full. The **reset dns forward table** command can delete all DNS entries.

Example

Clear DNS entries in the DNS table on the DNS proxy or DNS relay.

```
<Huawei> reset dns forward table
```

Related Topics

8.4.7 display dns forward table

8.4.31 reset dns statistics

Function

The **reset dns statistics** command clears statistics on DNS packets.

Format

reset dns statistics

Parameters

None

Views

User view

Default Level

3: Management level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The **reset dns statistics** command clears statistics on DNS packets, including the DNS IPv4 and IPv6 addresses. The cleared statistics cannot be restored.

Example

Clear statistics on DNS packets.

```
<Huawei> reset dns statistics
```

8.4.32 ssl-policy (ddns-policy-view)

Function

The **ssl-policy** command binds an SSL policy to a DDNS policy.

The **undo ssl-policy** command deletes an SSL policy from a DDNS policy.

By default, no SSL policy is bound to a DDNS policy.

Format

ssl-policy *policy-name*

undo ssl-policy

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an SSL policy bound to a DDNS policy.	The value is a string of 1 to 31 case-sensitive characters. It cannot contain a space or question mark (?).

Views

DDNS policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device functions as the DDNS client and communicates with a Siemens DDNS server, the device needs to encrypt packets using SSL. An SSL policy needs to be bound to the DDNS policy.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

An SSL policy has been created using the **ssl policy** *policy-name* [**type** { **client** | **server** }] command, and PKI domain to be used by the SSL policy has been configured using the **19.18.4 pki-realm** *realm-name* command.

A DDNS policy has been created using the **ddns policy** command and a URL has been configured for Siemens DDNS server using the **url** command.

Precautions

An SSL policy needs to be bound to the DDNS policy only when the device functions as the DDNS client and communicates with a Siemens DDNS server.

Example

Bind an SSL policy to a DDNS policy.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei] ssl policy siemens type client
[Huawei-ssl-policy-siemens] pki-realm abc
[Huawei-ssl-policy-siemens] quit
[Huawei] ddns policy huawei
[Huawei-ddns-policy-huawei] url https://192.168.36.67/nic/update?
group=med&user=huawei_test&password=12345&myip=192.168.19.2
[Huawei-ddns-policy-huawei] ssl-policy siemens
```

Related Topics

8.4.11 ddns policy

8.4.33 url (DDNS policy view)

8.4.33 url (DDNS policy view)

Function

The **url** command specifies the URL in DDNS update requests.

The **undo url** command deletes the URL in DDNS update requests.

By default, no URL is specified in DDNS update requests on the device.

Format

url *request-url* [**username** *username* **password** *password*]

undo url

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
request-url	Specifies the URL in DDNS update requests.	The value is a string case-sensitive characters without spaces and ranges from 20 to 256 characters. • If **username** *username* **password** *password* is not specified, the URL contains the user name and password, and their configurations are displayed in explicit text. For example, when the device uses TCP to communicate with www.oray.cn, the URL format of the DDNS update request is oray://huawei1:huawei2@phddnsdev.oray.net (**huawei1** indicates the user name and **huawei2** indicates the password). • If **username** *username* **password** *password* is specified, the URL only contains the fixed format <username>:<password>, not the user name and password. The user name and password are specified by **username** and **password**, and the password configuration is displayed in cipher text. For example, when the device uses TCP to communicate with www.oray.cn, the URL format of the

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		DDNS update request is oray://<username>:<password>@phddnsdev.oray.net (<username>:<password> is the fixed value).
username *username* **password** *password*	Specifies the user name and password for logging in to the DDNS server. **NOTE** To ensure password security, you are advised to run the **username** *username* **password** *password* command to configure a user name and password. The password information in the configuration file is displayed in cipher text.	• *username*: The value is a string of 1 to 32 case-sensitive characters without spaces. • *password*: The value is a string of 1 to 32 case-sensitive characters in explicit text or 48 to 68 case-sensitive characters in cipher text without spaces.

Views

DDNS policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a DDNS policy is created, enter the URL and specify a DDNS server in the URL.

The processes for the device to request DDNS updates from different DDNS servers are different; therefore, the URL configurations of DDNS servers are different.

- If **username** *username* **password** *password* is not specified,
  - When the device uses HTTP to communicate with the DDNS server provided at www.3322.org, the URL in a DDNS update request is:

    http://username:password@members.3322.org/dyndns/update?system=dyndns&hostname=<h>&myip=<a>
  - When the device uses HTTP to communicate with the DDNS server provided at www.dyndns.com, the URL in a DDNS update request is:

 Copyright © Huawei Technologies Co., Ltd.

http://username:password@update.dyndns.com/nic/update?hostname=<h>&myip=<a>

- When the device uses TCP to communicate with the DDNS server provided at www.oray.cn, the URL in a DDNS update request is:

  oray://username:password@phddnsdev.oray.net

- When the device uses HTTP to communicate with a common DDNS server, the URL in a DDNS update request is:

  http://username:password@merri.s.dnaip.fi/reg/h=<h>&a=<a>

  NOTE

  In the preceding URLs, *username* and *password* indicate the user name and password for logging in to the DDNS server. For example, in **http://huawei1:huawei2@merri.s.dnaip.fi/reg/h=<h>&a=<a>**, **huawei1** and **huawei2** indicate the user name and password for logging in to the DDNS server.

- When **username** *username* **password** *password* is specified,
  - When the device uses HTTP to communicate with the DDNS server provided at www.3322.org, the URL in a DDNS update request is:

    http://<username>:<password>@members.3322.org/dyndns/update?system=dyndns&hostname=<h>&myip=<a>

  - When the device uses HTTP to communicate with the DDNS server provided at www.dyndns.com, the URL in a DDNS update request is:

    http://<username>:<password>@update.dyndns.com/nic/update?hostname=<h>&myip=<a>

  - When the device uses TCP to communicate with the DDNS server provided at www.oray.cn, the URL in a DDNS update request is:

    oray://<username>:<password>@phddnsdev.oray.net

  - When the device uses HTTP to communicate with a common DDNS server, the URL in a DDNS update request is:

    http://<username>:<password>@merri.s.dnaip.fi/reg/h=<h>&a=<a>

    NOTE

    In the preceding URLs, <username> and <password> are fixed formats, which cannot be modified.

Where,

- The URL uses the default port number. The default port number of the DDNS server provided at www.oray.cn is 6060, the default HTTP port number is 80 and the default HTTPS port number is 443.
- The FQDN and IP address cannot be specified in the URL for the DDNS server provided at www.oray.cn. You can specify the FQDN when applying a DDNS policy on an interface. The IP address in the URL is the primary IP address of the interface to which a DDNS policy is applied.

  NOTE

  To prevent configuration errors, you are advised not to change <h> or <a> in the URL. The device automatically fills in <h> and <a> based on the FQDN specified when a DDNS policy is bound to the interface.

If you run the **url** command multiple times, only the latest configuration takes effect.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

In a URL, the user name and password are separated using :, the password and domain name are separated using @, and the domain name ends with /. Pay attention to the following points when using special characters in a URL.

Example

Specify the URL of the DDNS update request, in which the password is displayed in cipher text.

```
<Huawei> system-view
[Huawei] ddns policy mypolicy
[Huawei-ddns-policy-mypolicy] url "http://<username>:<password>@members.3322.org/dyndns/
update?system=dyndns&hostname=<h>&ip=<a>" username steven password nevets
```

Delete the specified URL of the DDNS update request.

```
<Huawei> system-view
[Huawei] ddns policy mypolicy
[Huawei-ddns-policy-mypolicy] undo url
```

Related Topics

8.4.3 display ddns policy

8.4.34 dns resolve policy a

Function

The **dns resolve policy a** command enables the DNS resolution policy function for class-A query requests and displays the DNS resolution policy view.

The **undo dns resolve policy a** command disables the DNS resolution policy function for class-A query requests.

By default, the DNS resolution policy function for class-A query requests is disabled.

Format

dns resolve policy a

undo dns resolve policy a

Parameters

None

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

To control access traffic, the administrator requires that users can access only some websites on which they can browse only texts or pictures. For example, in Wi-Fi connection scenarios such as in metro or on bus, passengers can access only specified websites. If they attempt to access other websites, their access requests are rejected or redirected to the specified websites.

The administrator can run the **dns resolve policy a** command to enable the DNS resolution policy function for class-A query requests. Then only some specified domain names can be resolved to meet the wireless connection requirements.

Follow-up Procedure

Run the **8.4.35 rule (DNS resolution policy view)** command to configure a DNS resolution rule.

Example

Enable the DNS resolution policy function for class-A query requests and display the DNS resolution policy view.

```
<Huawei> system-view
[Huawei] dns resolve policy a
```

8.4.35 rule (DNS resolution policy view)

Function

The **rule** command configures a DNS resolution rule.

The **undo rule** command deletes the DNS resolution rule.

By default, no DNS resolution rule is configured.

Format

rule *rule-id* [**if-match name** *hostname*] { **deny** | **permit** | **spoofing** *ip-address* }

undo rule *rule-id*

Parameters

Parameter	Description	Value
rule-id	Specifies the DNS resolution rule ID. A smaller value indicates a higher rule priority.	The value is an integer that ranges from 0 to 127.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
if-match name *hostname*	Specifies the domain name matching the DNS resolution rule. If this parameter is not configured, the DNS resolution rule matches all domain names.	The value is a string of 1 to 255 case-insensitive characters without spaces. It supports the digits 0-9, letters, and the following symbols: - _ . *. The symbol * indicates the wildcard that can only be prefixed to the domain name once. For example, ***.example.com** indicates that all host names in example.com are matched.
deny	Rejects the domain name resolution request matching the DNS resolution rule.	-
permit	Allows the domain name resolution request matching the DNS resolution rule.	-
spoofing *ip-address*	Specified the IP address of the spoofing response to the domain name resolution request matching the DNS resolution rule. A spoofing response uses the configured IP address as the domain name resolution result to respond to the domain name resolution request. The IP address may be directed to the local homepage (providing resources such as website navigation, local videos, and applications).	The value is in dotted decimal notation.

Views

DNS resolution policy view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the DNS resolution policy function is enabled, you need to configure a resolution rule in the DNS resolution policy view to implement domain name resolution, resolution prohibition, and spoofing response for a specified domain name.

The administrator can run the **rule** command to configure a specified DNS resolution rule.

Prerequisites

The DNS resolution policy function for class-A query requests has been enabled and the DNS resolution policy view has been displayed using the **dns resolve policy a** command.

Precautions

- If the rule ID specified in *rule-id* already exists, the new rule overwrites the original rule no matter whether the new and original rules conflict with each other.
- If the specified *rule-id* does not exist, create a rule using the specified *rule-id* and determine the rule insertion position based on the rule size.

Example

Add a rule with *rule-id* as 0 to the DNS resolution policy, and configure address spoofing based on the DNS resolution request for www.huawei.com with the spoofing response address 192.168.1.1.

```
<Huawei> system-view
[Huawei] dns resolve policy a
[Huawei-dns-resolve-policy-a] rule 0 if-match name www.huawei.com spoofing 192.168.1.1
```

8.5 NAT Configuration Commands

NOTE

By default, the route forwarding function is enabled on 8FE1GE and 24GE cards. These cards do not send received IP packets to the CPU when the IP packets are forwarded on a LAN card. In this way, NAT services configured on VLANIF interfaces do not take effect.

8.5.1 display firewall-nat session aging-time

Function

The **display firewall-nat session aging-time** command displays the timeout interval of entries in the firewall session table or NAT session table.

Copyright © Huawei Technologies Co., Ltd.

Format

display firewall-nat session aging-time

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays the timeout interval of sessions on the firewall session table or NAT session table.

Example

Display the timeout time of all entries in the session table.

```
<Huawei> display firewall-nat session aging-time
-------------------------------------------------
Protocol timeout:
  tcp protocol timeout         : 600   (s)
  tcp-proxy timeout            : 10    (s)
  http protocol timeout        : 120   (s)
  udp protocol timeout         : 120   (s)
  icmp protocol timeout        : 20    (s)
  dns protocol timeout         : 120   (s)
  ftp protocol timeout         : 120   (s)
  ftp-data protocol timeout    : 120   (s)
  rtsp protocol timeout        : 60    (s)
  rtsp-media protocol timeout  : 120   (s)
  sip protocol timeout         : 1800  (s)
  sip-media protocol timeout   : 120   (s)
User-define port timeout:
  tcp protocol port 10001      : 65535 (s)
  tcp protocol port 1          : 111   (s)
  tcp protocol port 4443       : 65535 (s)
  tcp protocol port 181        : 180   (s)
  udp protocol port 180        : 180   (s)
  udp protocol port 182        : 208   (s)
-------------------------------------------------
```

Table 8-47 Description of the **display firewall-nat session aging-time** command output

Item	Description
Protocol timeout	Session timeout interval of each protocol.
tcp protocol timeout	Timeout interval of TCP connections. The default value is 600, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
tcp-proxy timeout	Timeout interval of the TCP proxy. The default value is 10, in seconds.
udp protocol timeout	Timeout interval of UDP connections. The default value is 120, in seconds.
icmp protocol timeout	Timeout interval of ICMP connections. The default value is 20, in seconds.
dns protocol timeout	Timeout interval of the DNS protocol. The default value is 120, in seconds.
http protocol timeout	Timeout interval of the HTTP connections. The default value is 120, in seconds.
ftp protocol timeout	Timeout interval of the FTP control connection. The default value is 120, in seconds.
ftp-data protocol timeout	Timeout interval of the FTP connections. The default value is 120, in seconds.
sip protocol timeout	Timeout interval of the SIP protocol. The default value is 1800, in seconds.
sip-media protocol timeout	Timeout interval of the SIP media protocol. The default value is 120, in seconds.
rtsp protocol timeout	Timeout interval of the RTSP protocol. The default value is 60, in seconds.
rtsp-media protocol timeout	Timeout interval of the RTSP media protocol. The default value is 120, in seconds.
User-define port timeout	Timeout interval of a connection with a user-defined port as the destination port.
tcp protocol port *port-number*	Timeout interval of a data connection with a user-defined TCP port as the destination port. The default value is the default data connection timeout interval of the corresponding protocol, in seconds.
udp protocol port *port-number*	Timeout interval of a data connection with a user-defined UDP port as the destination port. The default value is the default data connection timeout interval of the corresponding protocol, in seconds.

Related Topics

8.5.15 firewall-nat session aging-time

Copyright © Huawei Technologies Co., Ltd.

8.5.2 display nat address-group

Function

The **display nat address-group** command displays the configuration of a NAT address pool.

Format

display nat address-group [*group-index*] [**verbose**]

Parameters

Parameter	Description	Value
group-index	Indicates the index of a NAT address pool.	The value must be an existing NAT address pool index.
verbose	Displays details about the NAT address pool.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can check the configuration and application of the NAT address pool.

Example

Display all the NAT address pools.

```
<Huawei> display nat address-group
NAT Address-Group Information:
 ----------------------------------------
 Index   Start-address      End-address
 ----------------------------------------
 1           10.1.1.1        10.1.1.10
 2         10.10.10.10       10.10.10.15
 ----------------------------------------
  Total : 2
```

Display the NAT address pool according to the index of the NAT address pool.

```
<Huawei> display nat address-group 1
 NAT Address-Group Information:
 ----------------------------------------
 Index   Start-address      End-address
 ----------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

```
1           10.1.1.1        10.1.1.10
---------------------------------------
 Total : 1
```

Display details about the NAT address pool.

```
<Huawei> display nat address-group 1 verbose
NAT Address-Group Information:
 ------------------------------------------------------------
 Index   Start-address      End-address  Ref-times  Ref-type
 ------------------------------------------------------------
 1           10.1.1.1        10.1.1.10          0      ----
 ------------------------------------------------------------
 Total : 1
```

Table 8-48 Description of the display nat address-group command output

Item	Description
NAT Address-Group Information	Information of the NAT address pool.
Index	Index of the NAT address pool.
Start-address	Start IP address of the NAT address pool.
End-address	End IP address of the NAT address pool
Ref-times	Number of times that a NAT address pool is referenced.
Ref-type	Mode in which the NAT address pool is referenced. • pat: translates the IP address and port information of data packets. • no-pat: only translates the IP addresses of data packets, not port information. • ----: indicates that the NAT address pool is not referenced.
Total	Number of NAT address pools.

Related Topics

8.5.16 nat address-group

8.5.3 display nat alg

Function

The **display nat alg** command displays whether NAT application level gateway (ALG) is enabled for an application layer protocol.

Format

display nat alg

Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the status of NAT ALG.

```
<Huawei> display nat alg
NAT Application Level Gateway Information:
---------------------------------
 Application          Status
---------------------------------
 dns                  Disabled
 ftp                  Disabled
 rtsp                 Enabled
 sip                  Disabled
 pptp                 Disabled
---------------------------------
```

Table 8-49 Description of the display nat alg command output

Item	Description
NAT Application Level Gateway Information	Information of the NAT ALG.
Application	Application protocol type.
Status	Whether the NAT ALG function is enabled.

Related Topics

8.5.17 nat alg

8.5.4 display nat sip cac bandwidth information

Function

The **display nat sip cac bandwidth information** command displays the current total bandwidth and occupied bandwidth on the device.

Copyright © Huawei Technologies Co., Ltd.

Format

display nat sip cac bandwidth information [**verbose**]

Parameters

Parameter	Description	Value
verbose	Displays details about the current total bandwidth and occupied bandwidth.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display details about the current total bandwidth and occupied bandwidth on the device.

```
<Huawei> display nat sip cac bandwidth information verbose
--------------------------------------------------------------------------------
Total Bandwidth(Kbps)       Used Bandwidth(Kbps)
  3000                      1900
--------------------------------------------------------------------------------
Src-IP          Src-Port Dest-IP         Dest-Port Protocol Used Bandwidth(Kbps)
192.168.0.4     50       1.1.1.1         5060      udp      1900
--------------------------------------------------------------------------------
```

Table 8-50 Description of the display nat sip cac bandwidth information verbose command output

Item	Description
Total Bandwidth	Total bandwidth on the device, in Kbps. To configure the total bandwidth, run the **8.5.18 nat sip cac enable** command.
Used Bandwidth	Occupied bandwidth on the device, in Kbps.
Src-IP	Source IP address, that is, calling-party IP address.
Src-Port	Source port number, that is, calling-party port number.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Dest-IP	Destination IP address, that is, called-party IP address.
Dest-Port	Destination port number, that is, called-party port number.
Protocol	Corresponding protocol of the SIP calling, and the protocol can only be UDP.

Related Topics

8.5.17 nat alg

8.5.18 nat sip cac enable

8.5.5 display nat dns-map

Function

The **display nat dns-map** command displays the configuration of DNS mapping.

Format

display nat dns-map [*domain-name*]

Parameters

Parameter	Description	Value
domain-name	Specifies the valid domain name that can be resolved by the DNS server.	The value is a string of 1 to 255 case-insensitive characters without spaces. The string cannot contain the following characters: / : < > @ \ | % ' ".

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Copyright © Huawei Technologies Co., Ltd.

Example

Display the configuration of NAT DNS mapping.

```
<Huawei> display nat dns-map
 NAT DNS mapping information:
 Domain-name : www.huawei.com
 Global IP   : gigabitethernet0/0/1 (Real IP : 192.168.4.2)
 Global port : 2
 Protocol    : tcp

 Total : 1
```

Table 8-51 Description of the display nat dns-map command output

Item	Description
NAT DNS mapping information	Information of NAT DNS Mapping.
Domain-name	Domain name.
Global IP	IP address provided for external access.
Global port	Port number provided for external access.
Protocol	Type of the protocol carried over IP.
Total	Number of NAT DNS mapping information items.

Related Topics

8.5.19 nat dns-map

8.5.6 display nat filter-mode

Function

The **display nat filter-mode** command displays the current NAT filtering mode.

Format

display nat filter-mode

Parameters

None

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run this command to check the current NAT filtering mode. The modes include:

- endpoint-independent: independent of the external address and port.
- endpoint-dependent: dependent on the external address and independent of the port.
- endpoint-and-port-dependent: dependent on the external address and port.

Example

Display the current NAT filtering mode.

```
<Huawei> display nat filter-mode
Nat filter mode is : endpoint-independent
```

Table 8-52 Description of the display nat dns-map command output

Item	Description
Nat filter mode is	The current NAT filtering mode.

Related Topics

8.5.20 nat filter-mode

8.5.7 display nat outbound

Function

The **display nat outbound** command displays information about outbound NAT.

Format

display nat outbound [**acl** *acl-number* | **address-group** *group-index* | **interface** *interface-type interface-number* [*.subnumber*]]

Parameters

Parameter	Description	Value
acl *acl-number*	Displays the number of a basic ACL or an advanced ACL.	The value must be an existing ACL number.
address-group *group-index*	Displays the index of a NAT address pool.	The value must be an existing address pool index.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface *interface-type interface-number* [*.subnumber*]	Displays the type and number of an interface or a sub-interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display all information about outbound NAT.

```
<Huawei> display nat outbound
 NAT Outbound Information:
 ----------------------------------------------------------------------------
 Interface                Acl     Address-group/IP/Interface      Type
 ----------------------------------------------------------------------------
 GigabitEthernet0/0/2     2000                          1    no-pat
 ----------------------------------------------------------------------------
  Total : 1
```

Table 8-53 Description of the display nat outbound command output

Item	Description
Interface	Name of an interface.
Acl	Basic or advanced ACL that is in use.
Address-group/IP/ Interface	The index of a NAT address pool or IP address or loopback interface.
Type	Type of NAT. (If no NAT address pool is specified, the IP address of the interface is used as the translated IP address. That is, Easy IP is used.)
Total	Number of outbound NAT information items.

Related Topics

8.5.24 nat outbound

Copyright © Huawei Technologies Co., Ltd.

8.5.8 display nat overlap-address

Function

The **display nat overlap-address** command displays information about the mapping between the overlapped address pool and the temporary address pool.

Format

display nat overlap-address { *map-index* | **all** | **inside-vpn-instance** *inside-vpn-instance-name* }

Parameters

Parameter	Description	Value
map-index	Specifies the index of the mapping between the overlapped address pool and the temporary address pool.	The value must be an existing mapping index.
all	Displays the configuration of all the overlapped address pools.	-
inside-vpn-instance *inside-vpn-instance-name*	Displays the VPN instance of the private network.	The value is a string of 1 to 31 characters.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the configuration of all the overlapped address pools.

```
<Huawei> display nat overlap-address all
Nat Overlap Address Pool To Temp Address Pool Map Information:
 ------------------------------------------------------------------------------
 Id  Overlap-Address  Temp-Address    Pool-Length        Inside-VPN-Instance-Name
 ------------------------------------------------------------------------------
 1   10.2.2.2         10.3.10.10      255                cmml
```


Copyright © Huawei Technologies Co., Ltd.

```
--------------------------------------------------------------------------------
Total : 1
```

Table 8-54 Description of the display nat overlap-address command output

Item	Description
Id	Index of the mapping between the overlapped address pool and the temporary address pool.
Overlap-Address	Start IP address of the overlapped address pool.
Temp-Address	Start IP address of the temporary address pool.
Pool-Length	Length of the address pool.
Inside-VPN-Instance-Name	Name of the VPN instance of the private network.

Related Topics

8.5.26 nat overlap-address

8.5.9 display nat server

Function

The **display nat server** command displays the configuration of the NAT server.

Format

display nat server [**global** *global-address* | **inside** *host-address* [**vpn-instance** *vpn-instance-name*] | **interface** *interface-type interface-number* [*.subnumber*] | **acl** *acl-number*]

Parameters

Parameter	Description	Value
global *global-address*	Indicates the public address of the NAT server.	The value is in dotted decimal notation.
inside *host-address*	Indicates the private address of the NAT server.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Indicates the VPN instance name.	The value is a string of 1 to 31 characters.
interface *interface-type interface-number* [*.subnumber*]	Indicates the type and number of an interface or a sub-interface.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
acl *acl-number*	Indicates the number of an ACL.	The value is an integer that ranges from 2000 to 3999.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check whether the NAT server is configured correctly.

Example

Display the configuration of all NAT servers.

```
<Huawei> display nat server
  Nat Server Information:
  Interface  : GigabitEthernet1/0/0
  Global IP/Port     : 1.1.1.1/1~2
  Inside IP/Port     : 10.10.10.2~10.10.10.3/1
  Protocol : 6(tcp)
  VPN instance-name  : ----
  Acl number         : ----
  Vrrp id            : ----
  Description : ----

 Total :    1
```

Table 8-55 Description of the display nat server command output

Item	Description
Nat Server Information	Information of Nat Server.
Interface	Name of an interface.
Global IP/Port	Public IP address and port number.
Inside IP/Port	Private IP address and port number.
Protocol	Protocol number and protocol type.
VPN instance-name	Name of the VPN instance.
Acl number	Number of the ACL in the NAT server.
Vrrp id	VRRP ID.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Description	NAT description.
Total	Number of NAT servers.

Related Topics

8.5.27 nat server

8.5.10 display nat session

Function

The **display nat session** command displays the NAT mapping table.

Format

display nat session { **all** [**verbose**] | **number** }

display nat session protocol { *protocol-name* | *protocol-number* } [**source** *source-address* [*source-port*]] [**destination** *destination-address* [*destination-port*]] [**verbose**]

display nat session source *source-address* [*source-port*] [**destination** *destination-address* [*destination-port*]] [**verbose**]

display nat session destination *destination-address* [*destination-port*] [**verbose**]

Parameters

Parameter	Description	Value
all	Displays all entries in the NAT mapping table.	-
verbose	Displays detailed information about the NAT mapping table.	-
number	Displays the number of entries in the NAT mapping table.	-
protocol { *protocol-name* | *protocol-number* }	Displays the NAT mapping table with a specified protocol type or port number.	• The value of *protocol-name* can be icmp, tcp, or udp. • The value of *protocol-number* is an integer that ranges from 1 to 255.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
source *source-address* [*source-port*]	Specifies the source IP address and port number before the NAT translation.	• *source-address*: The value is in dotted decimal notation. • *source-port*: The value is an integer that ranges from 1 to 65535.
destination *destination-address* [*destination-port*]	Specifies the destination IP address and port number before the NAT translation.	• *destination-address*: The value is in dotted decimal notation. • *destination-port*: The value is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays information about the NAT mapping table. You can view information about all entries or display information by specifying keywords. The entries in a NAT mapping table are triggered by service packets. If the device does not receive any service packet, no entry is generated.

Example

Display details about all entries in the NAT mapping table.

```
<Huawei> display nat session all verbose
 NAT Session Table Information:

   Protocol          : TCP(6)
   SrcAddr  Port Vpn : 10.200.200.200 65532
   DestAddr Port Vpn : 10.100.100.100 1024
   Time To Live      : 60 s
   NAT-Info
     New SrcAddr     : 10.10.10.10
     New SrcPort     : 10240
     New DestAddr    : 10.30.30.30
     New DestPort    : 21

   Protocol          : UDP(6)
   SrcAddr  Port Vpn : 10.200.200.200 65532
   DestAddr Port Vpn : 10.100.100.100 1024
   Time To Live      : 60 s
   NAT-Info
     New SrcAddr     : 10.10.10.10
```

 Copyright © Huawei Technologies Co., Ltd.

```
    New SrcPort     : 10240
    New DestAddr    : 10.30.30.3
    New DestPort    : 21

Total : 2
```

Table 8-56 Description of the display nat session all verbose command output

Item	Description
NAT Session Table Information	Information of NAT mapping entries.
Protocol	Protocol type.
SrcAddr Port Vpn	Source address, service port number, and VPN instance name before the translation.
DestAddr Port Vpn	Destination address, service port number, and VPN instance name before the translation.
Time To Live	Time to live (TTL) of the mapping table entries.
NAT-Info	NAT information.
New SrcAddr	Source address after the translation.
New SrcPort	Source port number after the translation.
New DestAddr	Destination address after the translation.
New DestPort	Destination port number after the translation.
Total	Number of NAT mapping entries.

8.5.11 display nat static

Function

The **display nat static** command displays the configuration of static NAT.

Format

display nat static [**global** *global-address* | **inside** *host-address* [**vpn-instance** *vpn-instance-name*] | **interface** *interface-type interface-number* [*.subnumber*] | **acl** *acl-number*]

Parameters

Parameter	Description	Value
global *global-address*	Indicates the public address for static NAT.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
inside *host-address*	Indicates the private address for static NAT.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Indicates the name of the VPN instance.	The value is a string of 1 to 31 characters.
interface *interface-type interface-number* [*.subnumber*]	Indicates the type and number of an interface or a sub-interface.	-
acl *acl-number*	Indicates the number of an ACL.	The value is an integer that ranges from 2000 to 3999.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After static NAT is configured, you can use the display nat static command to view the configuration of static NAT.

Example

Display the global configuration of static NAT.

```
<Huawei> display nat static
  Static Nat Information:
  Interface  : GigabitEthernet1/0/0
    Global IP/Port     : 1.1.1.1/1~2
    Inside IP/Port     : 10.2.2.2~10.2.2.3/2
    Protocol : 6(tcp)
    VPN instance-name  : ----
    Acl number         : ----
    Vrrp id            : ----
    Netmask  : 255.255.255.255
    Description : ----

  Total :    1
```

Table 8-57 Description of the display nat static command output

Item	Description
Static Nat Information	Information of Static Nat.
Interface	Name of an interface.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Global IP/Port	Public IP address and port number.
Inside IP/Port	Private IP address and port number.
Protocol	Protocol number and protocol type.
VPN instance-name	Name of the VPN instance.
Acl number	Number of the ACL in the static NAT.
Vrrp id	VRRP ID.
Netmask	Network mask.
Description	NAT description.
Total	Number of static NATs.

Related Topics

8.5.29 nat static (interface view)

8.5.12 display nat static interface enable

Function

The **display nat static interface enable** command displays the interface enabled with the static NAT function.

Format

display nat static interface enable

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the interface enabled with the static NAT function.

Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display nat static interface enable
 Static Nat  enable  Information :
-------------------------------------------------
 interface Vlanif300
-------------------------------------------------
 Total : 1
```

Table 8-58 Description of the display nat static interface enable command output

Item	Description
Static Nat enable Information	Interface enabled with the static NAT function.
Total	Number of interfaces enabled with the static NAT function.

Related Topics

8.5.31 nat static enable

8.5.13 display nat mapping-mode

Function

The **display nat mapping-mode** command displays the NAT mapping mode.

Format

display nat mapping-mode

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After NAT mapping is configured, you can view the NAT mapping information. For example, you can view:

- Endpoint-independent mapping information about TCP packets.
- Endpoint-independent mapping information about UDP packets.
- Endpoint-independent mapping about TCP and UDP packets.

Copyright © Huawei Technologies Co., Ltd.

Example

Display NAT mapping information.

```
<Huawei> display nat mapping-mode
  NAT Mapping Mode Information:
-------------------------------------------------------------
nat mapping-mode endpoint-independent tcp
-------------------------------------------------------------
  Total : 1
```

Table 8-59 Description of display nat mapping-mode command output

Item	Description
NAT Mapping Mode Information	Information of the NAT mapping mode.
Total	Number of the NAT mapping mode.

Related Topics

8.5.32 nat mapping-mode

8.5.14 display nat mapping table

Function

The **display nat mapping table** command displays NAT mapping table information or the number of entries in the NAT table.

Format

display nat mapping table { **all** | **number** }

display nat mapping table inside-address *ip-address* **protocol** *protocol-name* **port** *port-number* [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
all	Displays information about all entries in the NAT mapping table.	-
number	Displays the number of entries in the NAT mapping table.	-
inside-address *ip-address*	Indicates the internal IP address of the server.	The value is in dotted decimal notation.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
protocol *protocol-name*	Indicates the protocol type.	The value can be tcp or udp.
port *port-number*	Indicates the protocol port number.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Indicates the VPN instance name.	The value is a string of 1 to 31 characters.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The display nat mapping table command displays information about all entries in a NAT table or the number of entries in the NAT table. You can also enter keywords to view a specified entry.

Example

Display the number of entries in the NAT table.

```
<Huawei> display nat mapping table number
 The total number of NAT dynamic mapping tables is: 1
```

Display information about all entries in the NAT table.

```
<Huawei> display nat mapping table all
 NAT Dynamic Mapping Table Information:

  Protocol            : UDP(17)
  InsideAddr  Port Vpn : 192.168.1.121   555
  GlobalAddr  Port     : 1.1.1.1         10491

  Protocol            : UDP(17)
  InsideAddr  Port Vpn : 192.168.1.119   555
  GlobalAddr  Port     : 2.2.2.2         23099

 Total : 2
```

Table 8-60 Description of the display nat mapping table command output

Item	Description
The total number of NAT dynamic mapping tables is	Number of NAT mapping tables.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
NAT Dynamic Mapping Table Information	Information of NAT mapping tables.
Protocol	Application protocol type.
InsideAddr Port Vpn	Private IP address, port number, and VPN instance name. **NOTE** If no VPN is configured, the VPN instance name is not displayed.
GlobalAddr Port	Public IP address and port number.
Total	Number of NAT mapping tables.

8.5.15 firewall-nat session aging-time

Function

The **firewall-nat session aging-time** command sets the timeout interval of each entry in the session table.

The **undo firewall-nat session aging-time** command restores the default timeout interval of each entry in the session table.

Format

firewall-nat session { { **dns** | **ftp** | **ftp-data** | **http** | **icmp** | **tcp** | **tcp-proxy** | **udp** | **sip** | **sip-media** | **rtsp** | **rtsp-media** | **pptp** | **pptp-data** } | { **tcp** | **udp** } **user-define** *port-number* } **aging-time** *time-value*

undo firewall-nat session { { **all** | **dns** | **ftp** | **ftp-data** | **http** | **icmp** | **tcp** | **tcp-proxy** | **udp** | **sip** | **sip-media** | **rtsp** | **rtsp-media** | **pptp** | **pptp-data** } | { **tcp** | **udp** } **user-define** *port-number* } **aging-time**

Parameters

Parameter	Description	Value
dns	Sets the timeout interval of the DNS protocol.	-
ftp	Sets the timeout interval of the FTP control connection.	-
ftp-data	Sets the timeout interval of the FTP connection.	-
http	Sets the timeout interval of the HTTP connection.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
icmp	Sets the timeout interval of the ICMP connection.	-
tcp	Sets the timeout interval of the TCP connection.	-
tcp-proxy	Sets the timeout interval of the TCP proxy.	-
udp	Sets the timeout interval of the UDP connection.	-
sip	Sets the timeout interval of the SIP connection.	-
sip-media	Sets the timeout interval of the SIP media protocol.	-
rtsp	Sets the timeout interval of the RTSP protocol.	-
rtsp-media	Sets the timeout interval of the RTSP media protocol.	-
pptp	Sets the timeout interval of the PPTP control connection.	-
pptp-data	Sets the timeout interval of the PPTP connection.	-
all	Restores the default timeout interval of all the preceding connections.	-
user-define *port-number*	Specifies the user-defined TCP or UDP port number and configures the timeout interval for all data connections with this port as the destination port. **NOTE** This parameter only supports NAT and does not support firewall.	The value is an integer that ranges from 1 to 65535.
aging-time *time-value*	Specifies the timeout interval value.	The value is an integer that ranges from 1 to 65535, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **firewall-nat session aging-time** command sets the timeout interval for sessions of each protocol or port. If an entry in a session table is not used within the specified period, the entry expires. For example, the user with IP address 10.110.10.10 initiates a TCP connection through port 2000. If the TCP connection is not used within the timeout interval, the system deletes the TCP connection.

The default session timeout interval of a port is the same as that of the corresponding protocol. The following table lists the default session timeout interval of each protocol.

Protocol	Default Session Timeout Interval
tcp	600 seconds
tcp-proxy	10 seconds
udp	120 seconds
icmp	20 seconds
dns	120 seconds
http	120 seconds
ftp	120 seconds
ftp-data	120 seconds
sip	1800 seconds
sip-media	120 seconds
rtsp	60 seconds
rtsp-media	120 seconds
pptp	600 seconds
pptp-data	600 seconds

NOTE

When configuring the timeout interval for all sessions with a user-defined port as the destination port, you cannot set the port number to a default port number of the preceding protocols.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

For some services such as voice service, increase the TCP/UDP timeout interval to prevent service interruption.

You can set the session timeout interval for a maximum of 24 ports on the device.

Example

Set the timeout interval of the DNS connection to 60 seconds.

```
<Huawei> system-view
[Huawei] firewall-nat session dns aging-time 60
```

Related Topics

8.5.1 display firewall-nat session aging-time

8.5.16 nat address-group

Function

The **nat address-group** command configures a NAT address pool.

The **undo nat address-group** command deletes a NAT address pool.

By default, no NAT address pool is configured.

Format

nat address-group *group-index start-address end-address*

undo nat address-group *group-index*

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
group-index	Specifies the index of a NAT address pool.	• The value on AR100, AR120, AR150, AR160, AR200 and AR1200 series is an integer that ranges from 0 to 7. • The value on AR2201-48FE, AR2202-48FE, AR2204E, AR2204-27GE, AR2204-27GE-P, AR2204E-D-27GE, and AR2204-51GE-P is an integer that ranges from 0 to 7. • The value on AR2204, AR2220E, AR2220, AR2240, and AR2240C is an integer that ranges from 0 to 255. • The value on AR3200 and AR3600 series is an integer that ranges from 0 to 255.
start-address	Specifies the start address of the address pool.	The value is in dotted decimal notation.
end-address	Specifies the end address of the address pool.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The address pool is a set of consecutive IP addresses. When a packet from the private network reaches the public network through address translation, the

 Copyright © Huawei Technologies Co., Ltd.

source address of the packet will be translated to another address by the address pool.

Precautions

The start IP address of the address pool must be smaller than or equal to the end IP address of the address pool and up to 255 IP addresses can be configured in the address pool.

Example

Configure an address pool ranging from 10.110.10.10 to 10.110.10.15, with the address pool index being 1.

```
<Huawei> system-view
[Huawei] nat address-group 1 10.110.10.10 10.110.10.15
```

Related Topics

8.5.2 display nat address-group

8.5.17 nat alg

Function

The **nat alg** command enables the NAT ALG function for application protocols.

The **undo nat alg** command disables the NAT ALG function for application protocols.

By default, NAT ALG is disabled.

Format

nat alg { **all** | *protocol-name* } **enable**

undo nat alg { **all** | *protocol-name* } **enable**

Parameters

Parameter	Description	Value
all	Enables the NAT ALG function for DNS, FTP, SIP, PPTP and RTSP.	-
protocol-name	Enables the NAT ALG function for the specified protocol type.	The value can be sippptp and rtsp.

Views

System view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

After the NAT ALG function is enabled for an application protocol, packets of the application protocol can traverse the public network through NAT. Otherwise, the application protocol cannot work normally.

Example

Enable the NAT ALG function for FTP.

```
<Huawei> system-view
[Huawei] nat alg ftp enable
```

Disable the NAT ALG function for FTP.

```
<Huawei> system-view
[Huawei] undo nat alg ftp enable
```

Related Topics

8.5.13 display nat mapping-mode

8.5.18 nat sip cac enable

Function

The **nat sip cac enable** command enables the function of call admission control and configures the total bandwidth of the device to limit the SIP call bandwidth.

The **undo nat sip cac enable** command disables the function of call admission control and cancels the configuration of total bandwidth. The SIP call bandwidth is not limited.

The default bandwidth of a device is 0, and the call bandwidth is not limited.

Format

nat sip cac enable bandwidth { *bandwidth-value* | **percent** *value* **interface** *interface-type interface-number* [*.subnumber*] }

undo nat sip cac enable

Parameters

Parameter	Description	Value
bandwidth *bandwidth-value*	Specifies the total bandwidth of the device.	The value is an integer that ranges from 1 to 4294967295, in kbit/s.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
percent *value*	Specifies the total bandwidth on the device, which is a percentage of the bandwidth on SIP outgoing interface.	The value is an integer that ranges from 1 to 100.
interface *interface-type interface-number* [*.subnumber*]	Specifies the SIP outgoing interface type and number. • *interface-type* specifies the interface type. • *interface-number* [*.subnumber*] specifies the interface number.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a SIP server is deployed on the public network and SIP phones in public and private networks are interconnected, the call quality is affected if the bandwidth on the NAT device is insufficient. You can enable call admission control (CAC) and set the total bandwidth on the NAT device to limit the bandwidth of SIP calls. If the bandwidth of a SIP exceeds the specified value, the SIP call is rejected.

Example

Set the total bandwidth of the device to 2000 kbit/s to limit the call bandwidth.

```
<Huawei> system-view
[Huawei] nat sip cac enable bandwidth 2000
```

Set the total bandwidth on the device to 10% of the bandwidth on GE1/0/0 to limit the call bandwidth.

```
<Huawei> system-view
[Huawei] nat sip cac enable bandwidth percent 10 interface gigabitethernet 1/0/0
```

Related Topics

8.5.4 display nat sip cac bandwidth information

 Copyright © Huawei Technologies Co., Ltd.

8.5.19 nat dns-map

Function

The **nat dns-map** command configures a mapping entry from the domain name to the public IP address, port number, and protocol type.

The **undo nat dns-map** command deletes a mapping entry from the domain name to the public IP address, port number, and protocol type.

By default, no mapping entry is configured.

Format

nat dns-map *domain-name* { *global-address* | **interface** *interface-type interface-number* [*.subnumber*] } *global-port protocol-name*

undo nat dns-map *domain-name* { *global-address* | **interface** *interface-type interface-number* [*.subnumber*] } *global-port protocol-name*

Parameters

Parameter	Description	Value
domain-name	Specifies a valid domain name that can be resolved by the DNS server.	The value is a string of 1 to 255 case-insensitive characters without spaces. The domain name of each level contains a maximum of 63 characters. Domain names of different levels are separated by periods (.) and contain a maximum of 255 characters. The string cannot contain the following characters: / : < > @ \ | % ' ".
global-address	Specifies a valid IP address provided for external access.	The value is in dotted decimal notation.
interface *interface-type interface-number* [*.subnumber*]	Specifies the type and number of an interface or a sub-interface.	-
global-port	Specifies the port number of the service provided for external access.	The value is an integer that ranges from 1 to 65535.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
protocol-name	Specifies the protocol carried over IP.	The value can be tcp and udp.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use this command to configure the mapping from the domain name to the public IP address, port number, and protocol type for internal hosts. In this manner, internal hosts can differentiate and access corresponding internal servers according to domain names when no DNS server is deployed on the private network.

By default, DNS mapping is not configured. In this case, after the external DNS server resolves public IP addresses from domain name requests of internal hosts, the internal hosts can be mapped to only one internal server. In addition, internal hosts cannot differentiate and access corresponding internal servers according to domain names.

Follow-up Procedure

Run the **nat alg dns enable** command to enable the DNS NAT ALG function. The NAT ALG function allows hosts on a private network to access servers on the private network through the external DNS server.

Example

Configure a mapping entry from a domain name to public IP address, port number, and protocol type.

```
<Huawei> system-view
[Huawei] nat dns-map www.test.com 10.1.1.1 2012 tcp
```

Related Topics

8.5.5 display nat dns-map

8.5.20 nat filter-mode

Function

The **nat filter-mode** command sets the NAT filtering mode.

Copyright © Huawei Technologies Co., Ltd.

The default NAT filtering mode is **endpoint-and-port-dependent**.

Format

nat filter-mode { **endpoint-dependent** | **endpoint-independent** | **endpoint-and-port-dependent** }

Parameters

Parameter	Description	Value
endpoint-dependent	Indicates the NAT filtering mode dependent on the external address and independent of the port.	-
endpoint-independent	Indicates the NAT filtering mode independent of the external address and port.	-
endpoint-and-port-dependent	Indicates the NAT filtering mode dependent on the external address and port.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

NAT filtering allows applications using the STUN and TURN technologies to traverse the NAT server.

NAT is performed on the traffic from the external network to the internal network:

- If the NAT filtering mode is set to endpoint-independent, the system uses "destination IP address+destination port number+protocol number" as the key to search the mapping table. If a corresponding entry is found, the system generates a reverse mapping entry. The destination address and port in the entry are the IP address and port number on the internal network.
- If the NAT filtering mode is set to endpoint-dependent, the system uses "source IP address+destination IP address+destination port number+protocol

 Copyright © Huawei Technologies Co., Ltd.

number" as the key to search the mapping table. If a corresponding entry is found, the system generates a reverse mapping entry. The behavior in the reverse mapping entry is the same as the behavior in the mapping table entry.

- If the NAT filtering mode is set to endpoint-and-port-dependent, the system uses "source IP address+source port number+destination IP address +destination port number+protocol number" as the key to search the mapping table. If a corresponding entry is found, the system generates a reverse mapping entry. The behavior in the reverse mapping entry is the same as the behavior in the mapping table entry.

You can change the NAT filtering mode only when no traffic is transmitted between the external network and internal network.

Example

Set the NAT filtering mode independent of the external address and port.

```
<Huawei> system-view
[Huawei] nat filter-mode endpoint-independent
```

Related Topics

8.5.6 display nat filter-mode

8.5.21 nat inside priority enable

Function

The **nat inside priority enable** command enables the NAT service to have a higher priority than routing service.

The **undo nat inside priority enable** command disables the NAT service priority function and restores the priority of routing service.

By default, the routing service has a higher priority.

Format

nat inside priority enable

undo nat inside priority enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Application Scenario

You can run this command to specify whether the NAT service or routing service has a higher priority. If the NAT service has a higher priority, NAT is performed for traffic entering the device before routing. If the routing service has a higher priority, traffic is routed before NAT. This function is applicable to multi-uplink scenarios. For example, in a dual-uplink scenario, when you run the **nat static** command in the interface view or **nat static** in the system view on the master device to configure a static mapping between a public IP address and a private IP address, a user network route (UNR) is generated. When you run the **ip route-static** command in the system view, a static route from the public IP address to the private IP address is configured. By running the preceding two commands, you expect that NAT can be performed on traffic entering the device and a backup route is available. A static route has a higher priority than that of the UNR. Therefore, the static route that is configured later overwrites the UNR, and NAT and route backup cannot be implemented on the device at the same time. To resolve this problem, run the **nat inside priority enable** command to enable the NAT service to take precedence over the routing service so that the device performs NAT on traffic before routing it.

Prerequisites

The static mapping from the private IP address to the public IP address has been configured. Two NAT methods are available to configure the static mapping from a private IP address to a public IP address:

- Run the **nat static (interface view)** command in the interface view to configure the static mapping between a private IP address and a public IP address.
- Run the **nat static (system view)** command in the system view to configure one-to-one NAT between private addresses and public addresses. Then run the **nat static enable** command in the interface view to enable the static NAT function.

Example

Enable the NAT service to have a higher priority than the routing service.

```
<Huawei> system-view
[Huawei] nat inside priority enable
```

8.5.22 nat log-format elog

Function

The **nat log-format elog** command sets the NAT log format to eLog. The logs are generated in the format specified by the eLog server.

The **undo nat log-format elog** command changes the current NAT log format from eLog to a common format.

By default, a common format is used as the NAT log format.

Copyright © Huawei Technologies Co., Ltd.

Format

nat log-format elog

undo nat log-format elog

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

In the scenario where connection between the device and eLog server is required, the device must send log packets in the specified format to the eLog server to establish the connection. You can run the **nat log-format elog** or **undo nat log-format elog** command to set the log format to eLog or a common format.

Example

Set the NAT session log format to eLog.

```
<Huawei> system-view
[Huawei] nat log-format elog
```

Set the NAT session log format to a common format.

```
<Huawei> system-view
[Huawei] undo nat log-format elog
```

Related Topics

19.8.55 firewall log session nat enable

8.5.23 nat miss forward deny

Function

The **nat miss forward deny** command enables a device to discard the packets that do not match the ACL rules bound to NAT.

The **undo nat miss forward deny** command disables a device from discarding the packets that do not match the ACL rules bound to NAT.

By default, the function of discarding the packets that do not match the ACL rules bound to NAT is disabled on a device.

Format

nat miss forward deny

 Copyright © Huawei Technologies Co., Ltd.

undo nat miss forward deny

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After an ACL is associated with an NAT address pool, the device translates the source address of a data packet matching the ACL into an IP address in the NAT address pool. You can run the **nat miss forward deny** command to enable the function of discarding the packets that do not match the ACL rules bound to NAT.

After this command is run, packets are discarded if the number of session entries exceeds the upper limit.

Example

Enable the device to discard the packets that do not match the ACL rules bound to NAT.

```
<Huawei> system-view
[Huawei] nat miss forward deny
```

8.5.24 nat outbound

Function

The **nat outbound** command associates an ACL with a NAT address pool. In this manner, the addresses specified in the ACL can be translated using the NAT address pool.

The **undo nat outbound** command disables outbound NAT.

By default, outbound NAT is disabled.

Format

nat outbound *acl-number* **address-group** *group-index* [**no-pat**][**vrrp** *vrrpid*]

undo nat outbound *acl-number* **address-group** *group-index* [**no-pat**][**vrrp** *vrrpid*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL.	The value is an integer that ranges from 2000 to 3999.
address-group *group-index*	Indicates that the NAT address pool is used for address translation. If no NAT address pool is specified, the IP address of the interface is used as the translated IP address. That is, Easy IP is used.	• The value on AR100, AR120, AR150, AR160, AR200 and AR1200 series is an integer that ranges from 0 to 7. • The value on AR2201-48FE, AR2202-48FE, AR2204E, AR2204-27GE, AR2204-27GE-P, AR2204E-D-27GE, and AR2204-51GE-P is an integer that ranges from 0 to 7. • The value on AR2204, AR2220E, AR2220, AR2240, and AR2240C is an integer that ranges from 0 to 255. • The value on AR3200 and AR3600 series is an integer that ranges from 0 to 255.
no-pat	Indicates one-to-one NAT, that is, only the IP address in a datagram is translated and the port number is not translated.	-
vrrp *vrrpid*	Specifies the VRRP ID.	The value is an integer that ranges from 1 to 255.

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Use Scenario

After an ACL is associated with a NAT address pool, NAT translates the source IP address of a data packet matching the ACL to an IP address in the NAT address pool.

On the same interface, different IP addresses can be translated and associated. This interface usually connects to an ISP network and is the egress of the internal network.

NOTE

This command can only be used on Layer 3 interfaces, except the Loopback, Tunnel-Template, and NULL interfaces.

Precautions

On the Layer 2 interface card of the AR2220, AR2240, AR2240C, AR3200 series, 3600 series, NAT needs to be configured on the VLANIF interface. In this case, run the **set workmode lan-card l3centralize** command in the system view to enable centralized forwarding.

Example

Select the addresses from 1.1.1.1 to 1.1.1.3 to form NAT address pool 1, and configure the hosts in the network segment 10.110.10.0/24 to use the addresses in address pool 1 for many-to-one address translation (using TCP/UDP port information).

```
<Huawei> system-view
[Huawei] acl number 2001
[Huawei-acl-basic-2001] rule permit source 10.110.10.0 0.0.0.255
[Huawei-acl-basic-2001] quit
[Huawei] nat address-group 1 1.1.1.1 1.1.1.3
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] nat outbound 2001 address-group 1
```

Related Topics

8.5.7 display nat outbound

8.5.25 nat outbound (Easy-IP)

Function

The **nat outbound** command configures Easy IP.

The **undo nat outbound** command disables outbound NAT.

By default, Easy IP is disabled.

Format

nat outbound *acl-number* [**interface** *interface-type interface-number* [*.subnumber*]] [**vrrp** *vrrpid*]

undo nat outbound *acl-number* [**interface** *interface-type interface-number* [*.subnumber*]][**vrrp** *vrrpid*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL.	The value is an integer that ranges from 2000 to 3999.
interface *interface-type interface-number* [*.subnumber*]	Indicates that a specified interface address or a sub-interface is specified as the translated address.	-
vrrp *vrrpid*	Specifies the VRRP ID.	The value is an integer that ranges from 1 to 255.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Easy IP indicates that the IP address of the interface is used as the translated IP address.

NOTE

This command can only be used on Layer 3 interfaces, except the Loopback, Tunnel-Template, and NULL interfaces.

Only one command can be configured on an interface.

Example

Set the IP address of the interface to the translated IP address.

```
<Huawei> system-view
[Huawei] acl number 2001
[Huawei-acl-basic-2001] rule permit source 10.110.10.0 0.0.0.255
[Huawei-acl-basic-2001] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] nat outbound 2001
```

Related Topics

8.5.7 display nat outbound

Copyright © Huawei Technologies Co., Ltd.

8.5.26 nat overlap-address

Function

The **nat overlap-address** command configures the mapping between an overlapped address pool and a temporary address pool.

The **undo nat overlap-address** command deletes the mapping between an overlapped address pool and a temporary address pool.

By default, the mapping between an overlapped address pool and a temporary address pool is not configured.

Format

nat overlap-address *map-index overlappool-startaddress temppool-startaddress* **pool-length** *length* [**inside-vpn-instance** *inside-vpn-instance-name*]

undo nat overlap-address { *map-index* | **all** | **inside-vpn-instance** *inside-vpn-instance-name* }

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
map-index	Specifies the index of the mapping between the overlapped address pool and the temporary address pool.	• The value on AR100, AR120, AR150, AR160, AR200 and AR1200 series is an integer that ranges from 0 to 7. • The value on AR2201-48FE, AR2202-48FE and AR2204 is an integer that ranges from 0 to 7. • The value on AR2220E and AR2220 is an integer that ranges from 0 to 15. • The value on AR2204XE and AR2204XE-DC is an integer that ranges from 0 to 31. • The value on the AR2240 and AR3200 varies according to the SRU model: – SRU40 and SRU60: 0-15. – SRU80, SRU100, SRU100E, SRU200, SRU200E and SRU400: 0-31. • The value on AR3600 is an integer that ranges from 0 to 31.
overlappool-startaddress	Specifies the start address of the overlapped address pool. IP addresses of overlapped address pools must be different.	The value is in dotted decimal notation.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
temppool-startaddress	Specifies the start address of the temporary address pool. IP addresses of temporary address pools must be different.	The value is in dotted decimal notation.
pool-length *length*	Indicates the length of the address pool. The lengths of the overlapped address pool and the temporary address pool are the same and an address in the overlapped address pool maps an address in the temporary address pool.	The value is an integer that ranges from 1 to 255.
all	The configuration of all the overlapped address pools.	-
inside-vpn-instance *inside-vpn-instance-name*	Indicates the VPN instance of the private network.	The value is a string of 1 to 31 characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When IP addresses of internal hosts and external hosts are overlapped, you need to configure the mapping between the overlapped address pool and the temporary address pool. After the mapping is configured, the overlapped address is translated into a unique temporary address. The packets can be forwarded correctly. In addition, you need to configure outbound NAT to implement twice NAT.

Example

Configure the mapping between an overlapped address pool and a temporary address pool with the index being 1. The length of the overlapped address pool is 255, the overlapped address pool belongs to the VPN **huawei**, and the start

 Copyright © Huawei Technologies Co., Ltd.

address of the overlapped address pool is 10.10.10.1. The start address of the temporary address pool is 10.100.100.1.

```
<Huawei> system-view
[Huawei] ip vpn-instance huawei
[Huawei-vpn-instance-huawei] route-distinguisher 200:1
[Huawei-vpn-instance-huawei-af-ipv4]  quit
[Huawei-vpn-instance-huawei] quit
[Huawei] nat overlap-address 1 10.10.10.1 10.100.100.1 pool-length 255 inside-vpn-instance huawei
```

Related Topics

8.5.8 display nat overlap-address

8.5.27 nat server

Function

The **nat server** command defines a mapping table of internal servers so that external users can access internal servers through address and port translation.

The **undo nat server** command cancels the mapping table.

By default, no mapping table is configured.

Format

nat server protocol { **tcp** | **udp** } **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* [*.subnumber*] } *global-port* [*global-port2*] [**vrrp** *vrrpid*] **inside** *host-address* [*host-address2*] [*host-port*] [**vpn-instance** *vpn-instance-name*] [**acl** *acl-number*] [**description** *description*]

nat server [**protocol** { *protocol-number* | **icmp** | **tcp** | **udp** }] **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* [*.subnumber*] } [**vrrp** *vrrpid*] **inside** *host-address* [**vpn-instance** *vpn-instance-name*] [**acl** *acl-number*] [**description** *description*]

undo nat server protocol { **tcp** | **udp** } **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* [*.subnumber*] } *global-port* [*global-port2*] [**vrrp** *vrrpid*] **inside** *host-address* [*host-address2*] [*host-port*] [**vpn-instance** *vpn-instance-name*]

undo nat server [**protocol** { *protocol-number* | **icmp** | **tcp** | **udp** }] **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* [*.subnumber*] } [**vrrp** *vrrpid*] **inside** *host-address* [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
protocol	Indicates the protocol type.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
protocol-number	Specifies the protocol number.	The value is an integer that ranges from 1 to 255.
global	Configures external information about the NAT server.	-
icmp	Indicates that servers communicate with each other using ICMP.	-
tcp	Indicates that servers communicate with each other using TCP.	-
udp	Indicates that servers communicate with each other using UDP.	-
global-address	Specifies a valid IP address provided for external access.	The value is in dotted decimal notation.
inside	Configures internal information about the NAT server.	-
host-address	Specifies an IP address of the NAT server.	The value is in dotted decimal notation.
host-address2	Specifies the ending IP address of the private network.	The value is in dotted decimal notation.
global-port	Specifies the external service port number. You can use keywords to replace common port numbers. For example, the FTP port number is 21, so you can use the keyword **ftp**. If this parameter is not specified, the value of this parameter is 0. That is, any type of service can be provided.	The value is an integer that ranges from 0 to 65535.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
global-port2	Specifies the external service ending port number. You can use keywords to replace common port numbers. For example, the FTP port number is 21, so you can use the keyword **ftp**. If this parameter is not specified, the value of this parameter is 0. That is, any type of service can be provided.	The value is an integer that ranges from 0 to 65535.
host-port	Specifies the service port number provided by the NAT server. If this parameter is not specified, the value of this parameter is the same as the value of *global-port*.	The value is an integer that ranges from 0 to 65535.
vpn-instance *vpn-instance-name*	Specifies the name of a private network-side VPN instance.	The value is a string of 1 to 31 characters.
vrrp *vrrpid*	Specifies the VRRP ID. After NAT address pools are configured on devices in a VRRP group, both devices may perform NAT for packets, resulting in conflicts. You can specify **vrrp** *vrrpid* to configure the master device to perform NAT, preventing conflicts.	The value is an integer that ranges from 1 to 255.
acl *acl-number*	Indicates the number of an ACL.	The value is an integer that ranges from 2000 to 3999.
description *description*	Indicates the NAT description.	The value is a string of 1 to 255 case-sensitive characters. It can contain spaces.
current-interface	Indicates a public address as the current interface address.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface *interface-type interface-number* [*.subnumber*]	Indicates a public address as the interface address.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure an internal server so that the external network can access the server in an active manner. When a host on the public network sends a connection request to the public address (global-address) of the internal NAT server, the NAT server translates the destination address of the request into a private address (inside-address). The request is then forwarded to the server on the private network.

NOTE

- This command can only be used on Layer 3 interfaces, except the Loopback, Tunnel-Template, and NULL interfaces.
- When configuring an internal NAT server, ensure that *global-address* and *host-address* are different from IP addresses of ports and IP addresses in the user address pool.
- You can use the IP address of **current-interface** or **loopback** as the internal server's IP address.
- The **undo nat server** command does not delete mapping entries immediately. You can run the **8.5.34 reset nat session** command to delete mapping entries.
- Compared with static NAT, NAT Server translates only the IP address, but not the port number, when the private network initiatively accesses the public network.
- When you configure one-to-one NAT Server that borrows an interface IP address (no interface number is specified and the IP address is mapped to a private network address), other services enabled on the interface may become unavailable. Confirm your action before performing the configuration. If you want to enable other applications on the interface, add an ACL rule after the configuration to filter out the number of the interface on which the applications are enabled.

Precautions

The specified *global-port* or *host-port* cannot be used by other applications. Otherwise, the configuration does not take effect.

When specifying *global-port2* to configure multiple public ports, you must also specify *host-address2* to configure multiple private addresses and ensure that the number of ports is the same as that of private addresses.

If you need to map the private address of an internal server into the IP address of the public network interface when configuring this command on the public

 Copyright © Huawei Technologies Co., Ltd.

network interface, you must set the **current-interface** parameter to specify a global address as the current interface address.

If you specify **vrrp** *vrrpid* when configuring the **nat server** command on an interface, the interface must support the VRRP function.

The *vpn-instance-name* parameter in the command specifies a private network-side VPN instance and does not take effect on the *global-address* parameter. The **ip binding vpn-instance** *vpn-instance-name* command can be run in the interface view to bind a public network-side VPN instance to the interface.

Example

Add a NAT server and translate public address 1.1.1.1 of the TCP service to private address 192.168.0.1.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] nat server protocol tcp global 1.1.1.1 inside 192.168.0.1
```

Configure NAT server on the public network interface Gigabitethernet 0/0/1 to map TCP port 8080 in the private IP address 192.168.20.2 of an internal server into port 8080 in the IP address of Gigabitethernet 0/0/1.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] nat server protocol tcp global current-interface 8080 inside
192.168.20.2 8080
```

Add a NAT server, translate public address 1.1.1.1 of the TCP protocol to private address 192.168.0.1, and only allow users with public address 2.2.2.2 to access the intranet server using IP address 1.1.1.1.

```
<Huawei> system-view
[Huawei] acl 2001
[Huawei-acl-basic-2001] rule 5 permit source 2.2.2.2 0
[Huawei-acl-basic-2001] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] nat server protocol tcp global 1.1.1.1 inside 192.168.0.1 acl 2001
```

Related Topics

8.5.9 display nat server

8.5.34 reset nat session

8.5.28 nat session limit

Function

The **nat session limit** command configures the maximum number of NAT mapping entries that can be used by a user.

The **undo nat session limit** command deletes the setting of the maximum number of NAT mapping entries that can be used by a user.

By default, the maximum number of NAT mapping entries that can be used by a user is not configured.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Only V200R010C10 and later version support this function.

Format

nat session limit *limit-number* **per-ip** [**acl** *acl-number*]

undo nat session limit

Parameters

Parameter	Description	Value
limit-number	Specifies the maximum number of NAT mapping entries that can be used by a user.	The value is an integer ranging from 1 to 65535.
per-ip	Specifies the maximum number of NAT mapping entries that can be used by a user based on the user's source IP address.	-
acl *acl-number*	Specifies the number of an ACL.	The value is an integer ranging from 2000 to 3999.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Application Usage Scenario

Since terminals are vulnerable to network attacks on a complex network, the terminals under network attacks will occupy a large number of NAT mapping entries on the devices they connected to. Once the NAT mapping entries on the devices are exhausted, other terminals cannot access the Internet because no NAT mapping entry can be allocated to them. In this case, you can run the **nat session limit** command to set the maximum number of NAT mapping entries that can be used by users. When the number of NAT mapping entries created for a user exceeds the configured limit, the device does not generate new NAT mapping entries. As a result, denying the user's Internet access is restricted.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

- This command cannot be used together with other functions for creating flow tables, such as the firewall, IPS, and SAC. Otherwise, this command may not take effect.
- If an ACL is configured, ACL rule updates do not affect the maximum number of NAT mapping entries that can be used by a user.
- If an ACL is configured and the ACL rule defines **deny**, the number of NAT mapping entries that can be used by a user is not limited.
- The NAT session table created on the device before this command is run is not included in the statistics of NAT mapping entries.
- After an active/standby device switchover is performed, the devices clear the statistics of NAT mapping entries that have been collected before the switchover and re-collects the statistics.

Example

Set the maximum number of NAT mapping entries that can be created for a user's source IP address to 2000.

```
<Huawei> system-view
[Huawei] nat session limit 2000 per-ip
```

8.5.29 nat static (interface view)

Function

The **nat static** command configures the static mapping between a private IP address and a public IP address.

The **undo nat static** command deletes the static mapping between a private IP address and a public IP address.

By default, the static mapping between a private IP address and a public IP address is not configured.

Format

nat static protocol { **tcp** | **udp** } **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* [*.subnumber*] } *global-port* [*global-port2*] [**vrrp** *vrrpid*] **inside** *host-address* [*host-address2*] [*host-port*] [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**acl** *acl-number*] [**global-to-inside** | **inside-to-global**] [**description** *description*]

nat static [**protocol** { *protocol-number* | **icmp** | **tcp** | **udp** }] **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* [*.subnumber*] } [**vrrp** *vrrpid*] **inside** *host-address* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**acl** *acl-number*] [**global-to-inside** | **inside-to-global**] [**description** *description*]

nat static protocol { **tcp** | **udp** } **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* [*.subnumber*] } *global-port global-port2* [**vrrp** *vrrpid*] **inside** *host-address host-port host-port2* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**acl** *acl-number*] [**description** *description*]

undo nat static protocol { **tcp** | **udp** } **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* [*.subnumber*] } *global-port* [*global-*

 Copyright © Huawei Technologies Co., Ltd.

port2] [**vrrp** *vrrpid*] **inside** *host-address* [*host-address2*] [*host-port*] [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**global-to-inside** | **inside-to-global**]

undo nat static [**protocol** { *protocol-number* | **icmp** | **tcp** | **udp** }] **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* [*.subnumber*] } [**vrrp** *vrrpid*] **inside** *host-address* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**global-to-inside** | **inside-to-global**]

undo nat static protocol { **tcp** | **udp** } **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* [*.subnumber*] } *global-port global-port2* [**vrrp** *vrrpid*] **inside** *host-address host-port host-port2* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*]

Parameters

Parameter	Parameters	Value
protocol	Indicates the protocol.	-
protocol-number	Specifies a protocol number.	The value is an integer that ranges from 1 to 255.
icmp	Indicates address translation for ICMP packets.	-
tcp	Indicates address translation for TCP packets.	-
udp	Indicates address translation for UDP packets.	-
global	Configures public network information.	-
global-address	Specifies a public IP address.	The value is in dotted decimal notation.
global-port	Specifies the external service port number. If this parameter is not specified, the value of *global-port* is 0. That is, any type of service can be provided.	The value is an integer that ranges from 0 to 65535.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Parameters	Value
global-port2	Specifies a public end port number. If this parameter is specified, a range of consecutive port numbers are translated. If this parameter is not specified, only the port number *global-port* is translated.	The value is an integer that ranges from 0 to 65535.
inside	Configures private network information.	-
host-address	Specifies a private IP address.	The value is in dotted decimal notation.
host-address2	Specifies a private end IP address. If this parameter is specified, a range of consecutive IP addresses are translated. If this parameter is not specified, only the private IP address *host-address* is translated.	The value is in dotted decimal notation.
host-port	Specifies a service port number provided by private network devices. If this parameter is not specified, the value of *host-port* is the same as the value of *global-port*.	The value is an integer that ranges from 0 to 65535.
host-port2	Specifies a private end port number.	The value is an integer that ranges from 0 to 65535.
vpn-instance *vpn-instance-name*	Specifies the name of a private network-side VPN instance.	The value must be the name of an existing VPN instance.
vrrp *vrrpid*	Specifies a VRRP ID.	The value is an integer that ranges from 1 to 255.
netmask *mask*	Specifies the network mask for static NAT.	The value ranges from 255.255.255.0 to 255.255.255.255.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Parameters	Value
acl *acl-number*	Specifies the number of an ACL. You can use an ACL to control NAT implementation, ensuring that NAT is performed only for data packets that meet rules in the ACL.	The value is an integer that ranges from 2000 to 3999.
global-to-inside	Indicates static NAT in the direction from the public network to the private network. If unidirectional static NAT is not configured, IP addresses are translated in both directions.	-
inside-to-global	Indicates static NAT in the direction from the private network to the public network. If unidirectional static NAT is not configured, IP addresses are translated in both directions.	-
description *description*	Specifies the NAT description.	The value is a string of 1 to 255 case-sensitive characters without question marks (?). It can contain spaces.
current-interface	Specifies a public IP address as the IP address of the current interface.	-
interface *interface-type interface-number* [*.subnumber*]	Specifies a public IP address as the IP address of an interface or sub-interface. • *interface-type* specifies the interface type. • *interface-number* [*.subnumber*] specifies the number of the interface or sub-interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If devices on a private network allow access from devices on a public network through a fixed IP address, for example, a private server provides services to public network devices, the public network devices can access the server through a fixed public IP address. You can configure static NAT to translate the private IP address of the private server into the specified public IP address.

If a private server provides services to multiple public network segments, the private IP address of the server needs to be translated into multiple public IP addresses to ensure security. Generally, bidirectional translation between private and public IP addresses is implemented in static NAT. When a private server accesses a public network, the private IP address of the server cannot be translated into multiple public IP addresses. You can configure unidirectional static NAT to solve this problem. When a public network device accesses the private server, multiple public IP addresses are translated into the private IP address of the server using static NAT. When the private server accesses the public network, IP addresses are translated using outbound NAT.

Static NAT also supports IP address translation between network segments, that is, private IP addresses within a specified range and public IP addresses within a specified range can be translated into each other.

Precautions

After the **undo nat static** command is run on the device, static mapping entries on the device will not be cleared immediately. To clear static mapping entries immediately, run the **8.5.34 reset nat session** command.

When the *global-port*, *global-port2*, *host-port*, and *host-port2* parameters are specified to configure mappings between public and private port numbers, the number of public port numbers must be the same as the number of private port numbers and the port numbers must be mapped in sequence. For example, when **nat static protocol tcp global 1.1.1.1 11 20 inside 10.10.10.1 21 30** is configured, the public IP address 1.1.1.1 maps the private IP address 10.10.10.1, and public port numbers 11 to 20 map private port numbers 21 to 30 in sequence.

When *host-address2* is specified, *global-port2* and *host-port* must also be specified. The number of private addresses must be the same as the number of public port numbers. That is, the same public address maps different private addresses, and different public port numbers map the same private port number. For example, when **nat static protocol tcp global 1.1.1.1 11 12 inside 10.10.10.1 10.10.10.2 30** is configured, 1.1.1.1 and public port 11 map 10.10.10.1 and private port 30, and 1.1.1.1 and public port 12 map 10.10.10.2 and private port 30.

 Copyright © Huawei Technologies Co., Ltd.

If you specify **vrrp** *vrrpid* when configuring the **nat static** command on an interface, the interface must support the VRRP function.

The *vpn-instance-name* parameter in the command specifies a private network-side VPN instance and does not take effect on the *global-address* parameter. The **ip binding vpn-instance** *vpn-instance-name* command can be run in the interface view to bind a public network-side VPN instance to the interface.

If you specify *acl-number* when configuring multiple **nat static** commands on an interface, the ACL number specified in the commands must be the same. Otherwise, the configuration fails.

Example

Translate the combination of the public IP address 1.1.1.1 and port 200 in TCP packets to the combination of the private IP address 10.10.10.1 and port 300.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] nat static protocol tcp global 1.1.1.1 200 inside 10.10.10.1 300
```

Replace the IP address of packets from the VPN **huawei** and on the network segment 10.2.2.2 (24-bit mask) with the IP address on the network segment 10.3.3.3 (24-bit mask).

```
<Huawei> system-view
[Huawei] ip vpn-instance huawei
[Huawei-vpn-instance-huawei]  quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] nat static global 10.3.3.3 inside 10.2.2.2 vpn-instance huawei netmask 255.255.255.0
```

Related Topics

8.5.11 display nat static

8.5.34 reset nat session

8.5.30 nat static (system view)

Function

The **nat static** command configures one-to-one NAT between private addresses and public addresses in the system view.

The **undo nat static** command deletes one-to-one NAT configured between private addresses and public addresses in the system view.

By default, no one-to-one NAT is configured.

Format

nat static protocol { **tcp** | **udp** } **global** *global-address global-port* [*global-port2*] **inside** *host-address* [*host-address2*] [*host-port*] [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*]

nat static protocol { **tcp** | **udp** } **global interface loopback** *interface-number global-port* [*global-port2*] [**vpn-instance** *vpn-instance-name*] **inside** *host-*

 Copyright © Huawei Technologies Co., Ltd.

address [*host-address2*] [*host-port*] [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*]

nat static [**protocol** { *protocol-number* | **icmp** | **tcp** | **udp** }] **global** { *global-address* | **interface loopback** *interface-number* } **inside** *host-address* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*]

nat static protocol { **tcp** | **udp** } **global** *global-address global-port global-port2* **inside** *host-address host-port host-port2* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*]

nat static protocol { **tcp** | **udp** } **global interface loopback** *interface-number global-port global-port2* [**vpn-instance** *vpn-instance-name*] **inside** *host-address host-port host-port2* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*]

undo nat static protocol { **tcp** | **udp** } **global** *global-address global-port* [*global-port2*] **inside** *host-address* [*host-address2*] [*host-port*] [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*]

undo nat static protocol { **tcp** | **udp** } **global interface loopback** *interface-number global-port* [*global-port2*] [**vpn-instance** *vpn-instance-name*] **inside** *host-address* [*host-address2*] [*host-port*] [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*]

undo nat static [**protocol** { *protocol-number* | **icmp** | **tcp** | **udp** }] **global** { *global-address* | **interface loopback** *interface-number* } **inside** *host-address* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*]

undo nat static protocol { **tcp** | **udp** } **global** *global-address global-port global-port2* **inside** *host-address host-port host-port2* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*]

undo nat static protocol { **tcp** | **udp** } **global interface loopback** *interface-number global-port global-port2* [**vpn-instance** *vpn-instance-name*] **inside** *host-address host-port host-port2* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*]

Parameters

Parameter	Description	Value
protocol	Indicates a protocol.	-
protocol-number	Specifies the protocol number.	The value is an integer that ranges from 1 to 255.
global	Configures external address and port number.	-
global-address	Specifies the public IP address for NAT.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
inside	Configures internal address and port number.	-
host-address	Specifies the private IP address for NAT.	The value is in dotted decimal notation.
host-address2	Specifies the ending IP address of the private network.	-
global-port	Specifies the external service port number. If this parameter is not specified, the value of this parameter is 0. That is, any type of service can be provided.	The value is an integer that ranges from 0 to 65535.
global-port2	Specifies the external service ending port number.	The value is an integer that ranges from 0 to 65535.
host-port	Specifies the service port number provided by the server. If this parameter is not specified, the value of this parameter is the same as the value of *global-port*.	The value is an integer that ranges from 0 to 65535.
host-port2	Specifies a private end port number.	The value is an integer that ranges from 0 to 65535.
icmp	Indicates that servers communicate with each other using ICMP.	-
tcp	Indicates that servers communicate with each other using TCP.	-
udp	Indicates that servers communicate with each other using UDP.	-
vpn-instance *vpn-instance-name*	Indicates the VPN instance name.	The value is a string of 1 to 31 characters.
netmask *mask*	Indicates the network mask for static NAT.	The value ranges from 255.255.255.0 to 255.255.255.255.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
description *description*	Indicates the NAT description.	The value is a string of 1 to 255 characters. The character string is case sensitive. It can contain spaces but cannot contain the question mark (?).
interface loopback *interface-number*	Indicates a public address as the loopback interface address.	The value is an integer that ranges from 0 to 1023.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Static NAT indicates that a private address is statically bound to a public address when NAT is performed. The public IP address in static NAT is only used for translation of the unique and fixed private IP address of a host.

Static PAT indicates that a combination of the private address of a host, TCP/UDP protocol number, and internal port number is statically bound to a combination of the public address, TCP/UDP protocol number, and external port number. The public IP address in static PAT can be used for translation of multiple private addresses.

Using static NAT or PAT, hosts on the private network and hosts on the public network can access each other.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- If you run the **undo nat static** command, static mapping entries are not immediately deleted. To clear static mapping entries, run the **8.5.34 reset nat session** command.
- When the *global-port*, *global-port2*, *host-port*, and *host-port2* parameters are specified to configure mappings between public and private port numbers, the number of public port numbers must be the same as the number of private port numbers and the port numbers must be mapped in sequence. For example, when **nat static protocol tcp global 1.1.1.1 11 20 inside 10.10.10.1 21 30** is configured, the public IP address 1.1.1.1 maps the private IP address 10.10.10.1, and public port numbers 11 to 20 map private port numbers 21 to 30 in sequence.

  When *host-address2* is specified, *global-port2* and *host-port* must also be specified. The number of private addresses must be the same as the number of public port numbers. That is, the same public address maps different private addresses, and different public port numbers map the same private port number. For example, when **nat static protocol tcp global 1.1.1.1 11 12 inside 10.10.10.1 10.10.10.2 30** is configured, 1.1.1.1 and public port 11 map 10.10.10.1 and private port 30, and 1.1.1.1 and public port 12 map 10.10.10.2 and private port 30.
- **nat static protocol** { **tcp** | **udp** } **global interface loopback** *interface-number global-port* [*global-port2*] [**vpn-instance** *vpn-instance-name*] **inside** *host-address* [*host-address2*] [*host-port*] [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*]

  In the command, the first *vpn-instance-name* parameter specifies the VPN instance bound to the loopback interface, and the second *vpn-instance-name* parameter specifies a private network-side VPN instance.
- If the **ip binding vpn-instance** *vpn-instance-name* command is run in the interface view to bind a public network-side VPN instance to the interface, the **nat static** command in the system view does not take effect. In this case, you need to run the **nat static** or **nat server** command in the interface view.

Example

Translate the combination of Loopback 4 interface address and port 43 in TCP packets to private address 192.168.2.55.

```
<Huawei> system-view
[Huawei] interface loopback 4
[Huawei-LoopBack4] ip address 192.168.8.8 24
[Huawei-LoopBack4] quit
[Huawei] nat static protocol tcp global interface loopback 4 43 inside 192.168.2.55 netmask 255.255.255.255
```

Related Topics

8.5.11 display nat static

8.5.34 reset nat session

8.5.31 nat static enable

Function

The **nat static enable** command enables static NAT on an interface.

The **undo nat static enable** command disables static NAT on an interface.

By default, static NAT on an interface is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Format

nat static enable

undo nat static enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Using the **nat static enable** command, you can enable static NAT on an interface.

NOTE

This command can only be used on Layer 3 interfaces, except loopback and NULL interfaces.

When enabling static NAT on a sub-interface, you must also enable the function on the main interface. Otherwise, the function does not take effect on the sub-interface.

Example

Enable static NAT on an interface.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] nat static enable
```

Related Topics

8.5.11 display nat static

8.5.32 nat mapping-mode

Function

The **nat mapping-mode** command sets the NAT mapping mode.

The **undo nat mapping-mode** command restores the NAT mapping mode.

The default NAT mapping mode is endpoint-and-port-dependent.

Format

nat mapping-mode endpoint-independent [*protocol-name* [**dest-port** *port-number*]]

 Copyright © Huawei Technologies Co., Ltd.

undo nat mapping-mode endpoint-independent [*protocol-name* [**dest-port** *port-number*]]

Parameters

Parameter	Description	Value
endpoint-independent	Indicates the endpoint-independent mode.	-
protocol-name	Indicates the protocol type.	The value can be tcp and udp.
dest-port *port-number*	Indicates the destination port. NAT is performed on only the packets of which destination ports are this specified port.	The value is an integer that ranges from 1 to 65535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The NAT function resolves the problem of IPv4 address shortage and improves network security. NAT implementation of different vendors may be different, so the applications using the STUN, TURN, and ICE technologies may fail to traverse the NAT devices of these vendors. These technologies are mainly used on the SIP proxy. NAT mapping enables these applications to traverse the NAT devices.

NAT mapping has the following modes:

- Endpoint-independent mapping: The NAT reuses the port mapping for subsequent packets sent from the same internal IP address and port to any external IP address and port.
- Address and port-dependent mapping: The NAT reuses the port mapping for subsequent packets sent from the same internal IP address and port to the same external IP address and port while the mapping is still active.

Example

Enable the endpoint-and-port-independent mapping mode for TCP packets.

```
<Huawei> system-view
[Huawei] nat mapping-mode endpoint-independent tcp
```

Enable the endpoint-and-port-independent mapping mode for TCP and UDP packets.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] nat mapping-mode endpoint-independent
```

Related Topics

8.5.13 display nat mapping-mode

8.5.33 port-mapping

Function

The **port-mapping** command configures the mappings between ports and application-layer protocols.

The **undo port-mapping** command deletes the mappings between ports and application-layer protocols.

Format

port-mapping { **dns** | **ftp** | **http** | **sip** | **rtsp** | **pptp** } **port** *port-number* **acl** *acl-number*

undo port-mapping { **all** | { **dns** | **ftp** | **http** | **sip** | **rtsp** | **pptp** } **port** *port-number* **acl** *acl-number* }

Parameters

Parameter	Description	Value
all	Deletes the mappings from all ports.	-
dns	Specifies the mapping between the DNS protocol and a port.	-
ftp	Specifies the mapping between the FTP protocol and a port.	-
http	Specifies the mapping between the HTTP protocol and a port.	-
sip	Specifies the mapping between the SIP protocol and a port.	-
rtsp	Specifies the mapping between the RTSP protocol and a port.	-
pptp	Specifies the mapping between the PPTP protocol and a port.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
port *port-number*	Specifies the port mapping to a protocol.	The value of *port-number* is an integer that ranges from 1 to 65535.
acl *acl-number*	Specifies the ACL that controls the packets to which port mapping is applied.	The value of *acl-number* is an integer that ranges from 2000 to 2999.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Port mapping enables a server to provide various application-layer services for external systems through non-well-known ports. For example, the well-known port of the HTTP service is port 80. After port mapping is configured on the firewall, the firewall can use a non-well-known port to provide the HTTP service.

Port mapping reduces attacks to a certain service on the server.

Example

Map the HTTP service to port 10 and apply ACL 2000 to control the packets to which the mapping takes effect.

```
<Huawei> system-view
[Huawei] acl 2000
[Huawei-acl-basic-2000] rule  permit
[Huawei-acl-basic-2000] quit
[Huawei] port-mapping http port 10 acl 2000
```

Related Topics

19.8.20 display port-mapping

8.5.34 reset nat session

Function

The **reset nat session** command deletes entries from the NAT mapping table.

Copyright © Huawei Technologies Co., Ltd.

Format

reset nat session { **all** | **transit interface** *interface-type interface-number*[*.subnumber*] }

reset nat session protocol { *protocol-name* | *protocol-number* } [**source** *source-address* [*source-port*]] [**destination** *destination-address* [*destination-port*]]

reset nat session source *source-address* [*source-port*] [**destination** *destination-address* [*destination-port*]]

reset nat session destination *destination-address* [*destination-port*]

NOTE

V200R010C10 and later versions support the **protocol**, **source**, and **destination** parameters.

Parameters

Parameter	Description	Value
all	Deletes all entries from the NAT mapping table.	-
transit	Deletes the entries of traffic passing a specified interface.	-
interface *interface-type interface-number*[*.subnumber*]	Indicates the type and number of an interface or a sub-interface.	-
protocol { *protocol-name* | *protocol-number* }	Deletes the NAT mapping table with a specified protocol type or port number.	• The value of *protocol-name* can be icmp, tcp, or udp. • The value of *protocol-number* is an integer that ranges from 1 to 255.
source *source-address* [*source-port*]	Specifies the source IP address and port number before the NAT translation.	• *source-address*: The value is in dotted decimal notation. • *source-port*: The value is an integer that ranges from 1 to 65535.
destination *destination-address* [*destination-port*]	Specifies the destination IP address and port number before the NAT translation.	• *destination-address*: The value is in dotted decimal notation. • *destination-port*: The value is an integer that ranges from 1 to 65535.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the configurations of **nat alg**, **nat server**, **nat static**, and **nat outbound** are changed, the packets are not forwarded based on new configurations. You can run the **reset nat session** command to make the new configurations take effect. This command can be used to delete all entries or the entries for a specified protocol type or the entries of traffic passing a specified interface from the NAT mapping table.

Precautions

- After this command is used, entries are deleted from the NAT mapping table and the NAT configurations are modified immediately.
- After this command is executed, you must wait at least 10 seconds if you need to run the command again; otherwise, an error message is displayed.
- If all entries are deleted, communication among certain sessions may be affected for a short period.

Example

Delete all entries from the NAT mapping table.

```
<Huawei> system-view
[Huawei] reset nat session all
Warning:The current all NAT sessions will be deleted.
Are you sure to continue?[Y/N] y
```

Delete entries from the NAT mapping table on port GigabitEthernet0/0/1.

```
<Huawei> system-view
[Huawei] reset nat session transit interface gigabitethernet 0/0/1
Warning:The current all NAT sessions transiting GigabitEthernet0/0/1 will be deleted.
Are you sure to continue?[Y/N] y
```

Delete the NAT mapping entries of TCP.

```
<Huawei> system-view
[Huawei] reset nat session protocol tcp
Warning:The current NAT sessions (protocol: tcp) will be deleted.
Are you sure to continue?[Y/N] y
```

Related Topics

8.5.10 display nat session

Copyright © Huawei Technologies Co., Ltd.

8.5.35 set nat-session self-healing enable

Function

The **set nat-session self-healing enable** command enables the self-healing function on the timer of a NAT module.

The **set nat-session self-healing disable** command disables the self-healing function on the timer of a NAT module.

By default, the self-healing function on the timer of a NAT module is disabled.

Format

set nat-session self-healing enable

set nat-session self-healing disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the running timer of a NAT module is faulty, the NAT service fails and the device cannot work properly. In this case, run the **set nat-session self-healing enable** command. After the self-healing function is enabled on the timer of a NAT module, the usage of the timer can be automatically detected. If the timer is faulty, you can reset the device to rectify the fault and ensure the proper running of the device.

Example

Enable the self-healing function on the timer of a NAT module.

```
<Huawei> system
[Huawei] set nat-session self-healing enable
```

8.5.36 tcp proxy

Function

The **tcp proxy** command enables the TCP proxy function.

The **undo tcp proxy** command disables the TCP proxy function.

By default, the TCP proxy function is disabled on the device.

 Copyright © Huawei Technologies Co., Ltd.

Format

tcp proxy *ip-address port-number* [**acl** *acl-number*]

undo tcp proxy

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address bound to the TCP proxy.	The value is in dotted decimal notation. The IP address can only be a unicast IP address on the local device.
port-number	Specifies the listening port of the TCP proxy.	The value is an integer that ranges from 1024 to 65000. This port number cannot be occupied by other modules.
acl *acl-number*	Specifies the number of an ACL.	The value is an integer that ranges from 3000 to 3999. It is recommended that ACL filtering be performed for the IP address of the TCP connection initiator.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the SIP ALG scenario, if a SIP data packet sent by the SIP client is too large to be sent to the SIP server at a time, the client divides the oversized SIP data packet into multiple small data packets and sends them to the SIP server. In this case, you need to enable the TCP proxy function on the device so that the device reassembles the received small data packets into the original SIP packet, performs NAT, and then forwards the packet to the SIP server.

The device listens to packets based on the specified IP address and port number after the TCP proxy function is enabled, and then sets up a TCP connection with

 Copyright © Huawei Technologies Co., Ltd.

host A that initiates a TCP connection. After successfully setting up the TCP connection, the device proactively sets up a TCP connection with host B which is the destination device of host A, ensuring that hosts A and B can communicate properly.

Precautions

After the TCP proxy function is disabled, the device deletes TCP connections set up with all hosts and the session table saved on the device. Run the **reset nat session all** command to delete all flow table information.

Example

Enable the TCP proxy function.

```
<Huawei> system-view
[Huawei] tcp proxy 10.1.1.1 3333
```

8.5.37 tcp proxy aging-time

Function

The **tcp proxy aging-time** command sets the aging time of a TCP connection set up by the TCP proxy.

The **undo tcp proxy aging-time** command restores the default aging time of a TCP connection set up by the TCP proxy.

By default, the aging time of a TCP connection set up by the TCP proxy is 120 seconds.

Format

tcp proxy aging-time *aging-time*

undo tcp proxy aging-time

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time of a TCP connection set up by the TCP proxy.	The value is an integer that ranges from 10 to 3600, in seconds.

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

In the SIP ALG scenario, if a SIP data packet sent by the SIP client is too large to be sent to the SIP server at a time, the client divides the oversized SIP data packet into multiple small data packets and sends them to the SIP server. In this case, you need to enable the TCP proxy function on the device so that the device reassembles the received small data packets into the original SIP packet, performs NAT, and then forwards the packet to the SIP server.

If the TCP proxy function is enabled, the device exchanges TCP keepalive packets with a host after it sets up a TCP connection with the host. If the device does not receive TCP keepalive packets from the host within the time three times the aging time, it automatically deletes the TCP connection and corresponding session entry.

Example

Set the aging time of a TCP connection set up by the TCP proxy to 240 seconds.

```
<Huawei> system-view
[Huawei] tcp proxy aging-time 240
```

8.6 UDP Helper Configuration Commands

8.6.1 display udp-helper port

Function

The **display udp-helper port** command displays the configured UDP ports to which packets need to be relayed on the device.

Format

display udp-helper port

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the configured UDP ports to which packets need to be relayed, run this command. If the UDP helper function is not enabled, this command does not display any information.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the UDP ports to which packets need to be relayed.

```
<Huawei> display udp-helper port
Udp-Port-Number       Description
------------------------------------------------------------
      1              TCP Port Service Multiplexer
     37              Time
     49              TAC Access Control System
     53              Domain Name Server
     69              Trivial File Transfer Protocol
    137              NETBIOS Name Service
    138              NETBIOS Datagram Service
```

Table 8-61 Description of the display udp-helper port command output

Item	Description
Udp-Port-Number	UDP ports to which packets need to be relayed. UDP ports are classified into the following types: • Well-known port: The well-known port numbers range from 0 to 1023. These ports are used by standard TCP/UDP protocols. • Registered port: The registered port numbers range from 1024 to 49151. They are vendor-specific ports. • Dynamic/Static port: The dynamic or static port numbers range from 49152 to 65535. These ports can be used as required and may conflict on a network. To configure the UDP ports, run the **8.6.5 udp-helper port** command.
Description	UDP port description. For details about port numbers, see RFC1700.

Related Topics

8.6.4 udp-helper enable

8.6.5 udp-helper port

8.6.2 display udp-helper server

Function

The **display udp-helper server** command displays statistics about packets relayed by UDP helper.

Copyright © Huawei Technologies Co., Ltd.

Format

display udp-helper server [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays statistics about UDP broadcast packets relayed on the specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays statistics about packets relayed by UDP helper. The statistics help you monitor the UDP helper function.

Example

Display statistics about packets relayed by UDP helper.

```
<Huawei> display udp-helper server
Server-interface          Server-Ip          packet-num
--------------------------------------------------------------------------
GigabitEthernet1/0/0      192.168.2.1        10
GigabitEthernet1/0/0.1    192.168.1.2        25
```

Table 8-62 Description of the display udp-helper server command output

Item	Description
Server-interface	Interface on which packets are relayed by UDP helper. To configure the interface, run the **8.6.6 udp-helper server** command in the interface view.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Server-Ip	Destination server address. To configure the destination server address, run the **8.6.6 udp-helper server** command in the interface view.
packet-num	Number of UDP packets sent to the destination server.

Related Topics

8.6.6 udp-helper server

8.6.3 reset udp-helper packet

Function

The **reset udp-helper packet** command clears statistics about packets relayed by UDP helper.

Format

reset udp-helper packet

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

This command clears statistics about packets relayed by UDP helper. Before collecting packet statistics in a certain period, run this command to clear existing statistics first.

NOTICE

UDP helper statistics cannot be restored after being cleared. Exercise caution when you run the **reset udp-helper packet** command.

Copyright © Huawei Technologies Co., Ltd.

Example

Clear statistics about packets relayed by UDP helper.

```
<Huawei> reset udp-helper packet
Warning: This command will delete the packet statistics of udp-helper.Continue?[Y/N]y
```

Related Topics

8.6.4 udp-helper enable
8.6.5 udp-helper port
8.6.6 udp-helper server
8.6.2 display udp-helper server

8.6.4 udp-helper enable

Function

The **udp-helper enable** command enables the UDP Helper function.

The **undo udp-helper enable** command disables the UDP Helper function.

By default, the UDP Helper function is disabled.

Format

udp-helper enable

undo udp-helper enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hosts on an enterprise intranet may need to obtain the network configuration or resolve host names by sending UDP broadcast packets to the server. If the host and the server are located in different broadcast domains, broadcast packets cannot reach the server and the host cannot obtain the configuration from the server. The router provides the UDP Helper function to solve this problem. UDP Helper can relay the UDP broadcast packets with specified destination ports. It converts the broadcast packets into unicast packets and sends the unicast packets to the specified destination servers.

 Copyright © Huawei Technologies Co., Ltd.

The packets that can be forwarded by UDP Helper must meet the following requirements:

- The destination MAC address is the broadcast MAC address (ffff-ffff-ffff).
- The destination IP address is the broadcast IP address (255.255.255.255) or a subnet broadcast IP address (for example, 192.168.255.255).
- The Time-to-Live (TTL) is larger than 1.
- The protocol type is UDP.
- The destination port is a specified UDP port.

Precautions

UDP Helper does not relay DHCP packets. That is, the destination port number cannot be 67 or 68. To relay DHCP packets, run the **dhcp select relay** command.

After the UDP Helper function is enabled, the router relays broadcast packets destined for the following UDP ports by default.

Table 8-63 The relation of default UDP port number with UDP Protocol

Protocol	UDP Port Number
Time Service	37
Terminal Access Controller Access Control System (TACACS)	49
Domain Name System (DNS)	53
Trivial File Transfer Protocol (TFTP)	69
NetBIOS Name Service (NetBIOS-NS)	137
NetBIOS Datagram Service (NetBIOS-DS)	138

After UDP Helper is disabled, all specified UDP ports and default ports are canceled.

NOTE

After the UDP Helper function is enabled, the router automatically relays the UDP broadcast packets on six default ports. If you want to relay the packets on only one default port, run the **undo udp-helper port** { **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** } command to disable packet relay on other five ports.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable UDP Helper.

```
<Huawei> system-view
[Huawei] udp-helper enable
```

Related Topics

8.3.28 dhcp select relay

8.6.5 udp-helper port

8.6.6 udp-helper server

8.6.3 reset udp-helper packet

8.6.2 display udp-helper server

8.6.5 udp-helper port

Function

The **udp-helper port** command specifies the UDP ports to which UDP broadcast packets are relayed.

The **undo udp-helper port** command deletes the UDP ports to which packets are relayed.

By default, no UDP port is specified. After UDP helper is enabled, the router relays broadcast packets destined for ports 37, 49, 53, 69, 137, and 138 by default.

Format

udp-helper port { *port-number* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }

undo udp-helper port { *port-number* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }

Parameters

Parameter	Description	Value
port-number	Specifies the UDP ports to which packets are relayed.	The value is an integer that ranges from 1 to 65535, excluding 67 and 68.
dns	Relays the UDP broadcast packets sent by DNS. The UDP port number is 53.	-
netbios-ds	Relays the UDP broadcast packets sent by NetBIOS-DS. The UDP port number is 138.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
netbios-ns	Relays the UDP broadcast packets sent by NetBIOS-NS. The UDP port number is 137.	-
tacacs	Relays the UDP broadcast packets sent by TACACS. The UDP port number is 49.	-
tftp	Relays the UDP broadcast packets sent by TFTP. The UDP port number is 69.	-
time	Relays the UDP broadcast packets sent by time service. The UDP port number is 37.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After UDP helper is enabled and the UDP ports are specified, the router relays the received UDP broadcast packets destined for the specified ports.

The **udp-helper port** command takes effect globally. That is, if the router is configured to relay packets destined for a UDP port, all the interfaces configured with the destination server address will relay such packets.

Precautions

UDP helper does not relay DHCP packets. That is, the destination port number cannot be 67 or 68. To relay DHCP messages, enable the DHCP relay function.

In addition to the 6 default ports that have UDP Helper enabled, another 10 destination ports can be specified.

Example

Configure the router to relay the broadcast packets destined for UDP port 100.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] udp-helper enable
[Huawei] udp-helper port 100
```

Related Topics

8.6.4 udp-helper enable

8.6.6 udp-helper server

8.6.3 reset udp-helper packet

8.6.2 display udp-helper server

8.6.6 udp-helper server

Function

The **udp-helper server** command configures the destination server to which UDP packets are relayed.

The **undo udp-helper server** command deletes the destination server to which UDP packets are relayed.

By default, no destination server is configured for UDP Helper.

Format

udp-helper server *ip-address*

undo udp-helper server [*ip-address*]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a destination server. The IP address can be a unicast address or a subnet broadcast address, but cannot be 255.255.255.255. Otherwise, the configuration fails.	The value is in dotted decimal notation.

Views

Interface view

Default Level

2: Configuration level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

If UDP Helper is enabled and the destination server is configured on an interface, when the interface receives the UDP broadcast packets destined for the specified port, it converts the broadcast packets into unicast packets with the destination address *ip-address* and sends them to the specified server.

Prerequisites

The UDP Helper function is enabled by the **8.6.4 udp-helper enable** command.

Precautions

- If multiple destination servers are configured on an interface, the router converts the broadcast packets into unicast packets and sends them to all these servers.
- When specifying the IP address of a destination server, ensure that the router has a reachable route to the network segment where the destination server is located. If no route is reachable, packets cannot be forwarded.
- When the **undo udp-helper server** command is used without parameter specified, all the configured destination servers on the interface are deleted.

Example

Configure destination server 10.1.1.2 on GE1/0/0.

```
<Huawei> system-view
[Huawei] udp-helper enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] udp-helper server 10.1.1.2
```

Related Topics

8.6.4 udp-helper enable

8.6.5 udp-helper port

8.6.3 reset udp-helper packet

8.6.2 display udp-helper server

8.7 IP Performance Configuration Commands

8.7.1 broadcast routing disable

Function

The **broadcast routing disable** command disables routing forwarding of broadcast packets.

The **undo broadcast routing disable** command enables routing forwarding of broadcast packets.

By default, routing forwarding of broadcast packets is enabled.

Copyright © Huawei Technologies Co., Ltd.

Format

broadcast routing disable

undo broadcast routing disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

A router forwards broadcast packets according to its IP routing table by default. Broadcast packets carry the destination MAC address of FFFF-FFFF-FFFF and a unicast destination IP address. If there are multiple paths from the source device to the destination device, broadcast packets will be forwarded along multiple paths. As a result, multiple copies of packets will reach the destination device. To ensure that the destination device receives only one copy of packets, run the **broadcast routing disable** command. This command will enable routing forwarding of broadcast packets on the routers along only one path.

Example

Disable routing forwarding of broadcast packets.

```
<Huawei> system-view
[Huawei] broadcast routing disable
```

8.7.2 clear ip df

Function

The **clear ip df** command enables an interface to fragment outgoing IP packets.

The **undo clear ip df** command disables an interface from fragmenting outgoing IP packets.

By default, an interface does not fragment outgoing IP packets.

Format

clear ip df

undo clear ip df

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

After forcible IP packet fragmentation is enabled on a device, the device sets the Don't Fragment (DF) field to 0 and fragments IP packets that meet the following conditions:

- The value of the DF field in the IP packet header is 1.
- The packet length is larger than the MTU value of the interface that sends the packets.

Example

Enable forcible fragmentation for outgoing packets on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] clear ip df
```

8.7.3 control-packet output car bypass

Function

The **control-packet output car bypass** command configures the control packets generated by the device not to support traffic policing function.

The **undo control-packet output car bypass** command configures the control packets generated by the device to support traffic policing function.

By default, control packets generated by the device do not support traffic policing function.

Format

control-packet { **bgp** | **icmp** | **igmp** | **ospf** | **pim** | **rip** | **snmp** | **ssh** | **telnet** | **udp** [*ip_address port*] | **other-protocols** } * **output car bypass**

control-packet all output car bypass

undo control-packet { **bgp** | **icmp** | **igmp** | **ospf** | **pim** | **rip** | **snmp** | **ssh** | **telnet** | **udp** [*ip_address port*] | **other-protocols** } * **output car bypass**

undo control-packet all output car bypass

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
bgp	Indicates BGP packets.	-
icmp	Indicates ICMP packets.	-
igmp	Indicates IGMP packets.	-
ospf	Indicates OSPF packets.	-
pim	Indicates PIM packets.	-
rip	Indicates RIP packets.	-
snmp	Indicates SNMP packets.	-
ssh	Indicates SSH packets.	-
telnet	Indicates Telnet packets.	-
udp	Indicates UDP packets.	-
ip_address	Indicates IPv4 address.	The value is in dotted decimal notation.
port	Indicates the port.	The value is an integer that ranges from 0 to 65535.
other-protocols	Indicates other control packets except BGP, ICMP, IGMP, OSPF, PIM, RIP, SNMP, SSH, Telnet, and UDP packets.	-
all	Indicates all control packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the enhanced forwarding function of the control packets generated by the device is enabled, you can run the **undo control-packet output car bypass** command to configures control packets generated by the device to support traffic policing function to apply QoS policies to different control packets.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The enhanced forwarding function of the control packets generated by the device has been enabled using the **8.7.29 ip soft-forward enhance enable** command.

Follow-up Procedures

After control packets generated by the device are configured to support traffic policing function, configure QoS policies to process different control packets. For details about traffic policing configuration, see Configuring Traffic Policing in *Huawei AR Series Access Routers Configuration Guide-QoS*.

Precautions

- Configuring control packets generated by the device to support traffic policing function may cause control packets to be discarded and affect user services.
- In versions earlier than V200R005C00, if the **8.7.29 ip soft-forward enhance enable** command has been executed to enable the enhanced forwarding function on the device, the device generates the configuration file of the **undo control-packet all output car bypass** command after the device is upgraded to V200R005C00.
- When **bgp**, **icmp**, **igmp**, **ospf**, **pim**, **rip**, **snmp**, **ssh**, **telnet**, **udp**, and **other-protocols** are specified in the **undo control-packet output car bypass** commands, the device generates a configuration file of the **undo control-packet all output car bypass** command. If the **control-packet output queue bypass** command is then executed to configure a specified type of control packets generated by the device not to support traffic policing function, the device does not generate the configuration file of the **undo control-packet all output car bypass** command but generates the configuration files of the control packets that are configured to support traffic policing function. For example, if BGP packets, ICMP packets, IGMP packets, OSPF packets, PIM packets, RIP packets, SNMP packets, SSH packets, and UDP packets generated by the device are configured not to support traffic policing function, the device generates the configuration files of the **undo control-packet telnet other-protocols output car bypass** commands.

Example

Configure BGP packets generated by the device to support traffic policing function.

```
<Huawei> system-view
[Huawei] undo control-packet bgp output car bypass
```

Related Topics

8.7.29 ip soft-forward enhance enable

8.7.4 control-packet output filter bypass

Function

The **control-packet output filter bypass** command configures the device not to discard generated control packets when the traffic policy and ACL-based simplified traffic policy contain the deny action.

Copyright © Huawei Technologies Co., Ltd.

The **undo control-packet output filter bypass** command configures the device to discard generated control packets when the traffic policy and ACL-based simplified traffic policy contain the deny action.

By default, the device does not discard generated control packets when the traffic policy and ACL-based simplified traffic policy contain the deny action.

Format

control-packet { **bgp** | **icmp** | **igmp** | **ospf** | **pim** | **rip** | **snmp** | **ssh** | **telnet** | **udp** [*ip_address port*] | **other-protocols** } * **output filter bypass**

control-packet all output filter bypass

undo control-packet { **bgp** | **icmp** | **igmp** | **ospf** | **pim** | **rip** | **snmp** | **ssh** | **telnet** | **udp** [*ip_address port*] | **other-protocols** } * **output filter bypass**

undo control-packet all output filter bypass

Parameters

Parameter	Description	Value
bgp	Indicates BGP packets.	-
icmp	Indicates ICMP packets.	-
igmp	Indicates IGMP packets.	-
ospf	Indicates OSPF packets.	-
pim	Indicates PIM packets.	-
rip	Indicates RIP packets.	-
snmp	Indicates SNMP packets.	-
ssh	Indicates SSH packets.	-
telnet	Indicates Telnet packets.	-
udp	Indicates UDP packets.	-
ip_address	Indicates IPv4 address.	The value is in dotted decimal notation.
port	Indicates the port.	The value is an integer that ranges from 0 to 65535.
other-protocols	Indicates other control packets except BGP, ICMP, IGMP, OSPF, PIM, RIP, SNMP, SSH, Telnet, and UDP packets.	-
all	Indicates all control packets.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the enhanced forwarding function is enabled for the control packets generated by the device, the device does not discard the control packets when the traffic policy and ACL-based simplified traffic policy contain the deny action. After the **undo control-packet output filter bypass** command is executed, the device is configured to discard generated control packets when the traffic policy and ACL-based simplified traffic policy contain the deny action and apply QoS policy to the control packets to meet different service requirements.

Prerequisites

The enhanced forwarding function of control packets generated by the device has been enabled using the **8.7.29 ip soft-forward enhance enable** command.

Follow-up Procedures

The packet filter action in the traffic policy or ACL-based simplified traffic policy has been set to deny.

Precautions

- Configuring the device to discard generated control packet when the traffic policy and ACL-based simplified traffic policy contain the deny action may affect user services.
- When **bgp**, **icmp**, **igmp**, **ospf**, **pim**, **rip**, **snmp**, **ssh**, **telnet**, **udp**, and **other-protocols** are specified in the **undo control-packet output filter bypass** commands, the device generates a configuration file of the **undo control-packet all output filter bypass** command. If the **control-packet output filter bypass** command is then executed to configure the device not to discard a specified type of control packets, the device does not generate the configuration file of the **undo control-packet all output filter bypass** command but generates the configuration files of the control packets that the device is configured to discard. For example, if the device is configured not to discard BGP packets, ICMP packets, IGMP packets, OSPF packets, PIM packets, RIP packets, SNMP packets, SSH packets, and UDP packets the device generates the configuration files of the **undo control-packet telnet other-protocols output filter bypass** commands.

Example

Configure the device to discard generated BGP packets when the traffic policy and ACL-based simplified traffic policy contain the deny action.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] undo control-packet bgp output filter bypass
```

Related Topics

8.7.29 ip soft-forward enhance enable

8.7.5 control-packet output queue bypass

Function

The **control-packet output queue bypass** command configures the control packets generated by the device not to support QoS queue functions.

The **undo control-packet output queue bypass** command configures the control packets generated by the device to support QoS queue functions.

By default, control packets generated by the device do not support QoS queue functions.

Format

control-packet { **bgp** | **icmp** | **igmp** | **ospf** | **pim** | **rip** | **snmp** | **ssh** | **telnet** | **udp** [*ip_address port*] | **other-protocols** } * **output queue bypass**

control-packet all output queue bypass

undo control-packet { **bgp** | **icmp** | **igmp** | **ospf** | **pim** | **rip** | **snmp** | **ssh** | **telnet** | **udp** [*ip_address port*] | **other-protocols** } * **output queue bypass**

undo control-packet all output queue bypass

Parameters

Parameter	Description	Value
bgp	Indicates BGP packets.	-
icmp	Indicates ICMP packets.	-
igmp	Indicates IGMP packets.	-
ospf	Indicates OSPF packets.	-
pim	Indicates PIM packets.	-
rip	Indicates RIP packets.	-
snmp	Indicates SNMP packets.	-
ssh	Indicates SSH packets.	-
telnet	Indicates Telnet packets.	-
udp	Indicates UDP packets.	-
ip_address	Indicates IPv4 address.	The value is in dotted decimal notation.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
port	Indicates the port.	The value is an integer that ranges from 0 to 65535.
other-protocols	Indicates other control packets except BGP, ICMP, IGMP, OSPF, PIM, RIP, SNMP, SSH, Telnet, and UDP packets.	-
all	Indicates all control packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the enhanced forwarding function of the control packets generated by the device is enabled, you can run the **undo control-packet output queue bypass** command to configures control packets generated by the device to support QoS queue functions (such as traffic shaping, congestion management, and congestion avoidance) to apply QoS policies to different control packets.

Prerequisites

The enhanced forwarding function of the control packets generated by the device has been enabled using the **8.7.29 ip soft-forward enhance enable** command.

Follow-up Procedures

After control packets generated by the device are configured to support QoS queue functions, configure QoS policies to process different control packets.

Precautions

- Configuring control packets generated by the device to support QoS queue functions may cause control packets to be discarded and affect user services.
- In versions earlier than V200R005C00, if the **8.7.29 ip soft-forward enhance enable** command has been executed to enable the enhanced forwarding function on the device, the device generates the configuration file of the **undo control-packet all output queue bypass** command after the device is upgraded to V200R005C00.
- When **bgp**, **icmp**, **igmp**, **ospf**, **pim**, **rip**, **snmp**, **ssh**, **telnet**, **udp**, and **other-protocols** are specified in the **undo control-packet output queue bypass**

Copyright © Huawei Technologies Co., Ltd.

commands, the device generates a configuration file of the **undo control-packet all output queue bypass** command. If the **control-packet output queue bypass** command is then executed to configure a specified type of control packets generated by the device not to support QoS queue functions, the device does not generate the configuration file of the **undo control-packet all output queue bypass** command but generates the configuration files of the control packets that are configured to support QoS queue functions. For example, if BGP packets, ICMP packets, IGMP packets, OSPF packets, PIM packets, RIP packets, SNMP packets, SSH packets, and UDP packets generated by the device are configured not to support QoS queue functions, the device generates the configuration files of the **undo control-packet telnet other-protocols output queue bypass** commands.

Example

Configure BGP packets generated by the device to support QoS queue functions.

```
<Huawei> system-view
[Huawei] undo control-packet bgp output queue bypass
```

Related Topics

8.7.29 ip soft-forward enhance enable

8.7.6 display forward pie counter

Function

The **display forward pie counter** command displays statistics on packets of the Packet Input Export (PIE) queue.

NOTE

Only the AR169EGW-L, AR169EW, AR161EW, and AR161EW-M1 support this command.

Format

display forward pie counter

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When a device receives a large number of burst packets, the CPU usage of the device increases sharply. If the number of burst packets is beyond the processing

 Copyright © Huawei Technologies Co., Ltd.

capacity of the CPU, excess packets are discarded, resulting in packet loss. You can run the **display forward pie counter** command to check whether packet loss occurs in the PIE queue and determine whether the CPU usage has reached the upper limit accordingly.

Example

Display PIE queue packet statistics.

```
<Huawei> display forward pie counter
PIE0: received packets :39                 received bytes :2496
      dropped packets :0                   dropped bytes :0
PIE1: received packets :3823330              received bytes :5606902818
      dropped packets :0                   dropped bytes :0
PIE2: received packets :65                 received bytes :4518
      dropped packets :0                   dropped bytes :0
PIE3: received packets :200                 received bytes :19348
      dropped packets :0                   dropped bytes :0
PIE4: received packets :1308                 received bytes :370543
      dropped packets :1                   dropped bytes :152
PIE5: received packets :0                  received bytes :0
      dropped packets :0                   dropped bytes :0
```

Table 8-64 Description of the **display forward pie counter** command output

Item	Description
PIE	PIE queue.
received packets	Number of packets received in the PIE queue.
received bytes	Number of bytes received in the PIE queue.
dropped packets	Number of packets discarded in the PIE queue.
dropped bytes	Number of bytes discarded in the PIE queue.

8.7.7 discard { ra | rr | srr | ts }

Function

The **discard { ra | rr | srr | ts }** command configures the device to discard the packets that contain the route alert option, route record option, source route option, or timestamp option on interfaces.

The **undo discard { ra | rr | srr | ts }** command configures the device to process the packets that contain the route alert option, route record option, source route option, or timestamp option on interfaces.

Copyright © Huawei Technologies Co., Ltd.

By default, the packets that contain the route option are not discarded.

Format

discard { ra | rr | srr | ts }

undo discard { ra | rr | srr | ts }

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

IP packets can carry route options including the route alert option (**ra**), route record option (**rr**), source route option (**srr**), and timestamp option (**ts**).

These route options are used to diagnose network paths and temporarily transmit special services. These options, however, may be used by attackers to spy on the network structure for initiating attacks. This degrades network security and device performance. To solve this problem, you can run the **discard { ra | rr | srr | ts }** command to configure the device to discard the IP packets that contain the route options.

NOTE

The **discard { ra | rr | srr | ts }** command only takes effect for the packets on inbound interfaces.

Example

Configure the device to discard the packets that contain the route alert option on the interface GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] discard ra
```

8.7.8 display icmp statistics

Function

The **display icmp statistics** command displays ICMP traffic statistics.

Format

display icmp statistics

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display ICMP traffic statistics.

```
<Huawei> display icmp statistics
  Input: bad formats          0          bad checksum            0
         echo                10          destination unreachable 0
         source quench       0           redirects               0
         echo reply          25          parameter problem       0
         timestamp request   0           information request      0
         mask requests       0           mask replies            0
         time exceeded       0           timestamp reply         0
         Mping request       0           Mping reply             0
  Output:echo                25          destination unreachable 0
         source quench       0           redirects               0
         echo reply          10          parameter problem       0
         timestamp request   0           information reply       0
         mask requests       0           mask replies            0
         time exceeded       0           timestamp reply         0
         Mping request       0           Mping reply             0
```

Table 8-65 Description of the display icmp statistics command output

Item	Description
Input	Received packets.
Output	Sent packets.
bad formats	Number of packets in incorrect format.
bad checksum	Number of packets with checksum errors.
echo	Number of echo request packets.
destination unreachable	Number of unreachable packets.
source quench	Number of source quench packets.
redirects	Number of redirection packets.
echo reply	Number of echo reply packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
parameter problem	Number of packets with incorrect parameters.
timestamp request	Number of timestamp request packets.
information request	Number of information request packets.
information reply	Number of information reply packets.
mask requests	Number of mask request packets.
mask replies	Number of mask reply packets.
time exceeded	Number of expired packets.
timestamp reply	Number of timestamp reply packets.
Mping request	Number of multicast ping request packets.
Mping reply	Number of multicast ping reply packets.

8.7.9 display ip socket

Function

The **display ip socket** command displays information about the created IPv4 socket.

Format

display ip [**ha**] **socket** [**monitor**] [**task-id** *task-id* **socket-id** *socket-id* | **socket-type** *socket-type*]

Parameters

Parameter	Description	Value
ha	Displays IPv4 socket information on the slave main control board.	-
monitor	Displays information about the socket monitor. Information about the socket monitor is displayed together with information about the socket. If no parameter is specified, this command displays information about all types of sockets.	-
task-id *task-id*	Displays socket information of the task with a specified ID.	The value must be an existing task ID.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
socket-id *socket-id*	Displays information about the socket with a specified ID.	The value must be an existing socket ID.
socket-type *socket-type*	Displays information about a socket of a specified type.	The value is an integer. **Table 8-66** shows the value range.

Table 8-66 Value range of **socket-type** *socket-type*

Value	Description
1	TCP socket
2	UDP socket
3	RAWIP socket
4	RAWLINK socket

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

A socket monitor monitors and records each connection. A RawLink also monitors interfaces. The socket monitor records specific protocol events that occur during operations. In addition, it logs information in the disk space.

The socket monitor is similar to a black box of the system. It records specific events that happen during system operations. When the system fails, you can use information recorded by the socket monitor to locate faults.

You can also set the filtering rules, such as the task ID, socket ID, and socket type so that only the information matching the rules is displayed. This reduces information output and helps you locate faults accurately and efficiently.

Example

Display information about the IP socket.

```
<Huawei> display ip socket monitor
SOCK_STREAM:
Task = VTYD(30), socketid = 1, Proto = 6,
LA = 0.0.0.0:23, FA = 0.0.0.0:0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_KEEPALIVE SO_LINGER SO_REUSEPORT SO_SENDVPNID(23553)
SO_SETKEEPALIVE SO_SETACL,
```

 Copyright © Huawei Technologies Co., Ltd.

```
socket state = SS_PRIV SS_ASYNC
                    Socket Monitor:
Asyn Que status:
 read = 0, write = 0, connect = 0, close = 0,
 peer close = 0, accept = 0, keep alive down = 0,
 cram time = 00H00M00S, lost msg = 0, msg type = 0x00000000;
Nothing else has been captured!
SOCK_DGRAM:
Task = DHCP(54), socketid = 2, Proto = 17,
LA = 0.0.0.0:67, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 41600, sb_cc = 0, rb_cc = 0,
socket option = SO_BROADCAST SO_REUSEPORT SO_UDPCHECKSUM SO_SENDVPNID(14849),
socket state = SS_PRIV
                    Socket Monitor:
Statistics:
 input packets = 6,recv packets = 6,output packets = 0;
Rcvbuf status:
 cram time = 00H00M00S: full times = 0,dropped packets = 0;
Asyn Que status:
 read = 0, write = 0, connect = 0, close = 0,
 peer close = 0, accept = 0, keep alive down = 0,
 smb input = 0, smb output = 0, smooth over = 0,
 cram time = 00H00M00S, lost msg = 0, msg type = 0x00000000;
```

Table 8-67 Description of the display ip socket command output

Item	Description
SOCK_STREAM	Socket types: • SOCK_STREAM • SOCK_DGRAM • SOCK_RAWLINK • SOCK_RAWIP
Task = VTYD(30)	Type and ID of the task that invokes the socket. For example, the task named VTYD uses the socket, with the task ID being 30.
socketid = 1	Socket ID.
Proto = 6	Protocol number.
LA = 0.0.0.0:23, FA = 0.0.0.0:0,	• LA: Local address/port number. • FA: Remote address/port number.
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,	• sndbuf: maximum socket send buffer size. The value is in bytes. • rcvbuf: maximum socket receive buffer size. The value is in bytes. • sb_cc: number of sent packets. The value is in bytes and is valid only when TCP caches data packets. • rb_cc: number of received packets. The value is in bytes.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
socket option = SO_ACCEPTCONN SO_KEEPALIVE SO_LINGER SO_REUSEPORT SO_SENDVPNID (23553) SO_SETKEEPALIVE SO_SETACL,	Set socket options: • SO_DEBUG: indicates that debugging is enabled. • SO_ACCEPTCONN: indicates that the socket is the server and is responsible for monitoring. • SO_REUSEADDR: indicates that addresses are overlapped. After the option is set, multiple identical addresses can be bound to an interface. • SO_KEEPALIVE: indicates that the keepalive timer starts after a TCP connection is set up. • SO_DONTROUTE: indicates that a socket must choose the direct route to the destination when setting up a connection. • SO_BROADCAST: indicates that an interface can send broadcast packets. • SO_REUSEPORT: indicates that interfaces are overlapped. After the option is set, multiple identical interfaces can be bound to the local interface. This option is often set on servers. • SO_UDPCHECKSUM: indicates that the socket calculates the checksum of UDP packets. • SO_SENDVPNID: indicates an exclusive option for VPNs. • SO_SETKEEPALIVE: indicates that the keepalive timer starts after a TCP connection is set up. • SO_SETACL: indicates that an ACL can be configured on the interface. • SO_USELOOPBACK: indicates that a socket can use a loopback interface to receive or send data. • SO_LINGER: indicates the time for closing a TCP connection. If the time is not set to 0, a TCP connection is closed after the timer expires. If the time is set to 0, a TCP connection is closed immediately. • SO_OOBINLINE: indicates out-band data. When receiving data, a socket processes the out-band data first.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• SO_SENDDATAIF: indicates that a socket uses the specified interface to receive or send data. • SO_SENDDATAIF_DONTSETTTL: indicates that a socket uses the specified interface to receive or send data but does not set the TTL value. • SO_SETSRCADDR: indicates that a socket sets the source address of outgoing packets. • SO_SENDBY_IF_NEXTHOP: indicates that a socket sets the outbound interface and next hop address of outgoing packets.
socket state = SS_PRIV SS_ASYNC	Socket status: • SS_NOFDREF: indicates that the socket ID is deleted. • SS_ISCONNECTED: indicates that a TCP connection is set up. • SS_ISCONNECTING: indicates that a TCP connection is being set up. • SS_ISDISCONNECTING: indicates that a TCP connection is being closed. • SS_CANTSENDMORE: indicates that a socket cannot send data. • SS_CANTRCVMORE: indicates that a socket cannot receive data. • SS_RCVMARK: indicates that a socket sets the receiving option in the received packet. • SS_NBIO: indicates that the type of a socket is non-blocking. • SS_ISCONFIRMING: indicates that the upper-layer application will complete processing a connection. • SS_BLOCKING: indicates that congestion occurs during packet receiving and sending. • SS_RECALL: indicates that the message notification method is set by an asynchronous socket. • SS_PRIV: indicates the option transferred from the Unix. The option is invalid in the current socket. • SS_ASYNC: indicates the status identifier of an asynchronous socket.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Asyn Que status	Current asynchronous queue status.
read=0	Number of messages read by the asynchronous queue is 0.
write=0	Number of messages written by the asynchronous queue is 0.
connect=0	Number of connection messages in the asynchronous queue is 0.
close=0	Number of messages about closed connections in the asynchronous queue is 0.
peer close=0	Number of messages about connections closed by the remote end in the asynchronous queue.is 0.
accept=0	Number of messages received by the asynchronous queue is 0.
keep alive down=0	Number of keepalivedown messages in the asynchronous queue is 0.
cram time=00H00M00S	Time for the asynchronous queue to become full is 00:00:00.
lost msg=0	Number of asynchronous messages discarded by the asynchronous queue is 0.
msg type	Current asynchronous message type.
smb input = 0	Number of times of notifying the application layer to read received packets on the backup board.
smb output = 0	Number of times of notifying the application layer to read sent packets on the backup board.
smooth over = 0	Number of times of notifying the application layer that the smoothing is over.

Related Topics

8.7.36 reset ip socket monitor

8.7.10 display ip socket register-port

Function

The **display ip socket register-port** command displays non-well-known port numbers that have been assigned to services on the device.

Copyright © Huawei Technologies Co., Ltd.

Format

display ip socket register-port

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

As defined in RFC standards, port numbers larger than 1024 are non-well-known port numbers and can be assigned to desired services, such as NQA and SSH services. However, a non-well-known port number can be assigned to only one service on the same device. If you assign a non-well-known port number to two or more services, this port number takes effect for only the latest configured service. As a result, the other services using this port number will fail.

Before you assign a non-well-known port number to a service, run the **display ip socket register-port** command to check non-well-known port numbers that have been assigned to other services, preventing service failures caused by conflicts of non-well-known port numbers.

Example

Display non-well-known port numbers that have been assigned to services on the device.

```
<Huawei> display ip socket register-port
Port      Task        Type
3232      mdt         UDP4
3503      MPLSFW      UDP4
3784      BFD         UDP4
4784      BFD         UDP4
31009     MPLSFW      UDP4
3232      mdt         UDP6
3503      MPLSFW      UDP6
3784      BFD         UDP6
4784      BFD         UDP6
31009     MPLSFW      UDP6
```

Table 8-68 Description of the **display ip socket register-port** command output

Item	Description
Port	Non-well-known port number that has been assigned to a service.
Task	Name of the task to which a non-well-known port number is assigned.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Type	Port type, including TCP and UDP.

8.7.11 display ip statistics

Function

The **display ip statistics** command displays IP traffic statistics.

Format

display ip statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

IP traffic statistics include statistics about received packets (including discarded packets that carry source-route options), sent packets, fragmented packets, and reassembled packets. If a large number of bad protocol and no route fields is displayed in the command output, the device receives a large volume of IP packets of unknown protocol types and IP packets for which no routes can be found. In this situation, the device may be attacked by the connected devices.

Example

Display IP traffic statistics.

```
<Huawei> display ip statistics
 Input:     sum                 49617      local               40133
            bad protocol            0      bad format              0
            bad checksum            0      bad options             0
            discard srr             0      discard rr              0
            discard ra              0      discard ts              0
            TTL exceeded            0
 Output:    forwarding              0      local               44518
            dropped                 0      no route                0
 Fragment:  input                   0      output                  0
            dropped                 0
            fragmented              0      couldn't fragment       0
 Reassembling:sum                   0      timeouts                0
```

 Copyright © Huawei Technologies Co., Ltd.

Table 8-69 Description of the display ip statistics command output

Item	Description
Input	Received packets.
sum	Total number of packets.
local	Number of packets sent to the upper-layer protocol.
bad protocol	Number of received IP packets of unknown protocol types. The protocol field in the IP header cannot be identified by the upper-layer protocol.
bad format	Number of packets in incorrect format.
bad checksum	Number of packets with checksum errors.
bad options	Number of packets with incorrect options.
discard srr	Number of discarded packets with source route options.
discard rr	Indicates the number of packets that are received and then discarded because of record-route options.
discard ra	Indicates the number of packets that are received and then discarded because of alert-route options.
discard ts	Indicates the number of packets that are received and then discarded because of time stamps options.
TTL exceeded	Number of packets discarded because the TTL expires.
Output	Sent packets.
forwarding	Number of forwarded packets.
local	Number of generated packets.
dropped	Number of discarded packets.
no route	Number of packets for which no correct route can be found, including the packets sent and forwarded by the local device.
Fragment	Number of packet fragments.
input	Number of received fragments.
output	Number of sent fragments.
dropped	Number of discarded fragments.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
fragmented	Number of successfully fragmented packets.
couldn't fragment	Number of packets that cannot be fragmented.
Reassembling:sum	Number of successfully reassembled fragments.
timeouts	Number of expired fragments.

Related Topics

5.1.9 display ip interface
8.7.38 reset ip statistics

8.7.12 display load-sharing

Function

The **display load-sharing** command displays the Unequal Cost Multiple Path (UCMP) configuration.

Format

display load-sharing [**vpn-instance** *vpn-instance*] **ip-address** *ip-address mask*

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters.
ip-address *ip-address*	Specifies destination IP address of an equal-cost route in the routing table. The destination IP address can be a network segment.	The value is in dotted decimal notation.
mask	Specifies the mask length in the routing table.	The value is an integer that ranges from 0 to 32.

Views

User view

Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Check the UCMP configuration.

```
<Huawei> display load-sharing vpn-instance 0 ip-address 3.3.3.3 32

------------------------Load Sharing Information------------------------
ECMP Index is 0
UCMP is Enabled
------------------------------------------------------------------------------
NextHop          BandWidth        State            Interface

40.1.1.2         1000             Active           GE1/0/0

30.1.1.2         2000             Active           Eth-Trunk1
```

Table 8-70 Description of the display load-sharing command output

Item	Description
ECMP Index	ECMP index, maintained by the system.
UCMP is Enabled	The UCMP function is enabled. To enable the UCMP function, run the **8.7.33 load-balance unequal-cost enable** command.
NextHop	IP address of the next hop in the route matching the destination IP address.
BandWidth	Bandwidth of the link involved in UCMP. To set the UCMP bandwidth, run the **8.7.34 load-balance bandwidth** command.
State	UCMP status: • Active • Inactive
Interface	Outbound interface in the route matching the destination IP address.

Related Topics

8.7.34 load-balance bandwidth

8.7.33 load-balance unequal-cost enable

Copyright © Huawei Technologies Co., Ltd.

8.7.13 display network status

Function

Running the **display network status** command, you can check the network status of a device.

Format

display network status { **all** | **tcp** | **udp** | **port** *port-number* }

Parameters

Parameter	Description	Value
all	Displays all the network information.	-
tcp	Displays TCP.	-
udp	Displays UDP.	-
port *port-number*	Specifies the number of an interface.	The value is an integer ranging from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display network status** command is used to check the network status, such as the running interfaces and services on the network. For example, when you find that an interface is being used by an unknown module during a security scan, run the command to check out the module.

Example

Display the IPv4 RawIP connection status.

```
<Huawei> display network status all
Proto Task/SockId Local Addr&Port         Foreign Addr&Port       State
TCP   VTYD/1      0.0.0.0:23             0.0.0.0:0               Listening
TCP   HTTP/2      0.0.0.0:80             0.0.0.0:0               Listening
TCP   HTTP/1      0.0.0.0:443            0.0.0.0:0               Listening
TCP   VTYD/59     192.168.50.166:23      10.135.19.141:60445     Established
TCP6  VTYD/2      ::->23                 ::->0                   Listening
UDP   AGNT/1      0.0.0.0:161            0.0.0.0:0
UDP   SLAG/1      0.0.0.0:1025           0.0.0.0:0
UDP   RDS /1      0.0.0.0:1812           0.0.0.0:0
UDP6  AGT6/1      ::->161                ::->0
UDP6  RDS /2      ::->1812               ::->0
```


Copyright © Huawei Technologies Co., Ltd.

Table 8-71 Description of the **display network status** command output

Item	Description
Proto Task/SockId	Protocol Task and Socket ID
Local Addr&Port	Local IP address and Port number
Foreign Addr&Port	Remote IP address and Port number
State	Connection status

8.7.14 display rawip statistics

Function

The **display rawip statistics** command displays RawIP traffic statistics.

Format

display rawip statistics [**verbose**]

Parameters

Parameter	Description	Value
verbose	Displays detailed RawIP traffic statistics based on the ICMP, OSPF, RSVP, and Others protocols.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The statistics about RawIP packets include the number of sent RawIP packets and the number of received RawIP packets.

RSVP, OSPF, and ICMP packets are encapsulated into RawIP packets to be sent. During the ping operation, for example, you can run the **display rawip statistics** command to view the number of RawIP packets sent by the local device to check whether the abnormality on the network is caused by abnormal sending and receiving of RawIP packets.

If you want to diagnose problems and monitor information of specific applications, configure **verbose** in the **display rawip statistics** command to

 Copyright © Huawei Technologies Co., Ltd.

display application-specific RawIP packet statistics. The applications can be ICMP, OSPF, RSVP, and others.

Precautions

The number of packets received by a router includes the number of forwarded packets, packets sent to the upper layer, and discarded packets.

RawIP traffic statistics are collected based on the well-known protocol number. The protocol number is identified by the protocol field in the IP packet header.

- The protocol number of ICMP statistics is 1.
- The protocol number of OSPF statistics is 89.
- The protocol number of RSVP statistics is 46.
- Statistics about packets with other protocol numbers are collected into the Others field.

Example

View the statistics about RawIP packets.

```
<Huawei> display rawip statistics
Received packets:
  dropped packets because the socket buffer is full   : 0
  dropped packets because no matching socket is found : 0

Sent packets:
  dropped packets : 0
```

Table 8-72 Description of the **display rawip statistics** command output

Item	Description
Received packets	Indicates the statistics about received packets.
dropped packets because the socket buffer is full	Indicates the number of RawIP packets that are discarded because the socket buffer is full.
dropped packets because no matching socket is found	Indicates the number of RawIP packets that are discarded because the socket of the receiver does not match with that of the sender.
Sent packets	Indicates the number of sent packets.
dropped packets	Indicates the number of discarded packets.

Display detailed RawIP traffic statistics.

```
<Huawei> display rawip statistics verbose
Received packets:
------------------------------------------------------------------
Application    Overflow        No Matching
------------------------------------------------------------------
ICMP           0               0
OSPF           0               0
RSVP           0               0
```

 Copyright © Huawei Technologies Co., Ltd.

```
Others        0              1
------------------------------------------------------------------------------

Sent packets:
------------------------------------------------------------------------------
Application    Dropped Packets
------------------------------------------------------------------------------
ICMP           0
OSPF           0
RSVP           0
Others         0
------------------------------------------------------------------------------
```

Table 8-73 Description of the display rawip statistics verbose command output

Item	Description
Received packets	Statistics on received packets.
Application	Application type.
Overflow	Number of RawIP packets discarded because the Socket buffer is full.
No Matching	Number of RawIP packets discarded because the receiver's Socket is mismatching.
ICMP	ICMP packets.
OSPF	OSPF packets.
RSVP	RSVP packets.
Others	Other types of packets.
Sent packets	Statistics about sent packets.
Dropped Packets	Number of discarded packets.

Related Topics

8.7.39 reset rawip statistics

8.7.15 display tcp statistics

Function

The **display tcp statistics** command displays TCP traffic statistics.

Format

display tcp statistics

Parameters

None

Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command displays TCP traffic statistics including different types of received and sent packets. For example, duplicate received packets and packets with checksum errors. In addition, connection-related statistics are displayed, for example, times of accepted connections, the number of retransmitted packets, and the number of keepalive packets.

Most of the preceding statistics are expressed in number of packets, and some of them are expressed in number of bytes.

Example

Display TCP traffic statistics.

```
<Huawei> display tcp statistics
Received packets:
    Total: 0
    Total(64bit high-capacity counter): 0
    packets in sequence: 0 (0 bytes)
    window probe packets: 0, window update packets: 0
    checksum error: 0, offset error: 0, short error: 0

    duplicate packets: 0 (0 bytes), partially duplicate packets: 0 (0 bytes)
    out-of-order packets: 0 (0 bytes)
    packets of data after window: 0 (0 bytes)
    packets received after close: 0

    ACK packets: 0 (0 bytes)
    duplicate ACK packets: 0, too much ACK packets: 0

Sent packets:
   Total: 0
    Total(64bit high-capacity counter): 0
    urgent packets: 0
    control packets: 0 (including 0 RST)
    window probe packets: 0, window update packets: 0

    data packets: 0 (0 bytes),    data packets retransmitted: 0 (0 bytes)
    ACK-only packets: 0 (0 delayed)

Other information:
   Retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
   Keep alive timeout: 0, keep alive probe: 0,     Keep alive timeout, so connections disconnected : 0
   Initiated connections: 0,     accepted connections: 0, established connections: 0
   Closed connections: 0 (    dropped: 0, initiated dropped: 0)
   Packets dropped with MD5 authentication: 0
   Packets permitted with MD5 authentication: 0
   Send Packets permitted with Keychain authentication: 0
   Receive Packets permitted with Keychain authentication: 0
   Receive Packets Dropped with Keychain authentication: 0
```

 Copyright © Huawei Technologies Co., Ltd.

Table 8-74 Description of the display tcp statistics command output

Item	Description
Received packets	Statistics about received packets.
Total	Total number of packets.
Total (64bit high-capacity counter)	Total number of packets, using the 64-bit counter.
packets in sequence (bytes)	Number of bytes in the packets that arrive in order.
window probe packets	Number of window probe packets.
window update packets	Number of window update packets.
checksum error	Number of packets with checksum errors.
offset error	Number of packets with offset errors.
short error	Number of packets whose length is too short.
duplicate packets (bytes)	Number of bytes in the duplicate packets.
partially duplicate packets (bytes)	Number of bytes in partially duplicate packets.
out-of-order packets (bytes)	Number of bytes in the out-of-order packets.
packets of data after window (bytes)	Number of bytes in the packets whose size is greater than the window size.
packets received after close	Number of packets that arrive after a connection is closed.
ACK packets (bytes)	Number of acknowledged packets, in bytes.
duplicate ACK packets	Number of re-acknowledged packets.
too much ACK packets	Number of acknowledged packets with no data sent.
Sent packets	Number of sent packets.
urgent packets	Number of urgent packets.
control packets (RST)	Number of control packets (RST packets).
data packets	Number of data packets.
data packets retransmitted (0 bytes)	Number of bytes in the retransmitted packets.
ACK only packets (delayed)	Number of acknowledged packets that are delayed.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Retransmitted timeout	Timeout interval of the retransmission timer.
connections dropped in retransmitted timeout	Number of connections discarded because the number of retransmission times exceeds the threshold.
Keep alive timeout	Timeout interval of the keepalive timer.
keep alive probe	Number of sent keepalive packets.
Keep alive timeout, so connections disconnected	Number of connections discarded because keepalive probe fails.
Initiated connections	Number of initiated connections.
accepted connections	Number of accepted connections.
established connections	Number of established connections.
Closed connections (dropped, initiated dropped)	Number of closed connections (number of discarded packets after a connection is set up or before a connection is set up).
Packets dropped with MD5 authentication	Number of packets that fail to pass MD5 authentication.
Packets permitted with MD5 authentication	Number of packets that pass MD5 authentication.
Send Packets permitted with Keychain authentication	Number of sent packets that carry keychain options.
Receive Packets permitted with Keychain authentication	Number of received packets that pass keychain authentication.
Receive Packets Dropped with Keychain authentication	Number of received packets that fail to pass keychain authentication.

Related Topics

8.7.16 display tcp status

8.7.16 display tcp status

Function

The **display tcp status** command displays current TCP connection status.

 Copyright © Huawei Technologies Co., Ltd.

Format

display tcp status [[**task-id** *task-id*] [**socket-id** *socket-id*] | [**local-ip** *ip-address*] [**local-port** *local-port-number*] [**remote-ip** *ip-address*] [**remote-port** *remote-port-number*]]

Parameters

Parameter	Description	Value
task-id *task-id*	Displays the TCP connection status of the task with a specified ID.	The value must be an existing task ID.
socket-id *socket-id*	Displays the TCP connection status of the socket with a specified ID.	The value must be an existing socket ID.
local-ip *ip-address*	Displays the TCP connection status of a specified local IP address.	The value is in dotted decimal notation.
local-port *local-port-number*	Displays the TCP connection status of a specified local port ID.	The value must be an existing local port ID.
remote-ip *ip-address*	Displays the TCP connection status a specified remote IP address.	The value is in dotted decimal notation.
remote-port *remote-port-number*	Displays the TCP connection status of a specified remote port ID.	The value must be an existing remote port ID.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The transmission control protocol defined in RFC 793 ensures high reliability of transmission between hosts. TCP provides reliable and connection-oriented services in full duplex mode. Run the **display tcp status** command to monitor the TCP connection status. The following information is displayed.

- ID of the TCP task control block.
- ID of the IPv4 TCP task and socket.
- Local IPv4 address and port ID.

 Copyright © Huawei Technologies Co., Ltd.

- Remote IPv4 address and port ID.
- ID of the VPN instance to which the TCP connection belongs.
- IPv4 TCP connection status.

You can set filtering rules based on the Task ID, socket ID, IP address and port number of the local device, and IP address and port number of the remote device so that only the information matching the rules is displayed. This prevents unnecessary information from being displayed and helps you locate faults accurately and efficiently.

Precautions

The command output is null if there is no TCP connection.

Example

Display the TCP connection status on the local device.

```
<Huawei> display tcp status
TCPCB    Tid/Soid Local Add:port       Foreign Add:port      VPNID  State
0a5d560c 30 /1    0.0.0.0:23           0.0.0.0:0             14849 Listening
```

Display the status of the TCP connection originated from the local IP address 0.0.0.0 and port 23.

```
<Huawei> display tcp status local-ip 0.0.0.0 local-port 23
TCPCB    Tid/Soid Local Add:port       Foreign Add:port      VPNID  State
0a5d560c 30 /1    0.0.0.0:23           0.0.0.0:0             14849 Listening
```

Display the status of the TCP connection originated from the local IP address 0.0.0.0 and port 24.

```
<Huawei> display tcp status local-ip 0.0.0.0 local-port 24
TCPCB    Tid/Soid Local Add:port       Foreign Add:port      VPNID  State
```

Table 8-75 Description of the display tcp status command output

Field	Description
TCPCB	ID of the TCP task control block.
Tid/Soid	Task ID and socket ID.
Local Add: port	IP address and port number of the local device. If the value of Local Add is 0.0.0.0, TCP connections of all IP addresses are monitored. If the value of port is 0, the TCP connection of all ports is monitored.
Foreign Add: port	IP address and port number of the remote device. If the value of Foreign Add is 0.0.0.0, the TCP connection of all IP addresses is monitored. If the value of port is 0, TCP connections of all ports are monitored.

 Copyright © Huawei Technologies Co., Ltd.

Field	Description
VPNID	ID of the VPN instance to which the TCP connection belongs. ● -1: indicates all VPNs. ● 0: indicates the public VPN. ● Other values: indicates the private VPN. The VPNID is defined by users.
State	TCP connection status: ● Closed: indicates that the TCP connection is closed. ● Listening: indicates that the TCP connection is being monitored. ● Syn_Rcvd: indicates that a packet with the SYN flag is received. ● Established: indicates that the TCP connection has been set up. ● Close_Wait: indicates that a user sends a packet with the FIN flag to the server to close the TCP connection in Established state. The server then sends an ACK packet to the user after receiving the packet and enters the Close_Wait state. ● Fin_Wait1: indicates that a user sends a packet with the FIN flag to the server to close the TCP connection and enter this state. ● Fin_Wait2: indicates that a user receives an ACK packet that responds to the sent packet with the FIN flag. ● Time_Wait: indicates that TCP enters this state after the TCP connection is closed. When TCP has been in Time_Wait state two times the lifetime of the longest packets, records about the closed connection are deleted. ● Closing: indicates that the user and server close the TCP connection simultaneously.

8.7.17 display udp statistics

Function

The **display udp statistics** command displays UDP traffic statistics.

Format

display udp statistics

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command displays UDP traffic statistics including different types of received and sent packets. For example, packets with checksum errors. In addition, connection-related statistics are displayed, for example, the number of broadcast packets. The preceding statistics are expressed in number of packets.

Example

Display UDP traffic statistics.

```
<Huawei> display udp statistics
Received packets:
   Total: 0
   Total(64bit high-capacity counter): 0
   checksum error: 0
   shorter than header: 0
   data length larger than packet: 0
   unicast(no socket on port): 0
   broadcast/multicast(no socket on port): 0
   not delivered, input socket full: 0
   input packets missing pcb cache: 0

Sent packets:
   Total: 0
   Total(64bit high-capacity counter): 0
```

Table 8-76 Description of the display udp statistics command output

Item	Description
Received packet: Total: Total (64bit high-capacity counter):	Total number of received UDP packets. Total number of received UDP packets (using the 64-bit counter).
checksum error:	Number of packets with checksum errors.
shorter than header:	Number of packets whose length is shorter than the packet header.
data length larger than packet:	Number of packets whose data length is greater than the packet length.
unicast (no socket on port):	Number of unicast packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
broadcast/multicast (no socket on port):	Number of broadcast and multicast packets.
not delivered, input socket full:	Number of packets that are not sent out because the socket buffer is full.
input packets missing pcb cache:	Number of sent packets that are not found in the PCB cache.
Sent packets: Total: Total (64bit high-capacity counter):	Total number of sent UDP packets. Total number of sent UDP packets (using the 64-bit counter).

Related Topics

8.7.41 reset udp statistics

8.7.18 icmp blackhole unreachable send

Function

The **icmp blackhole unreachable send** command enables the terminal access to send a Destination Unreachable ICMP packet to an initiator when a tracert packet matches an IPv4 blackhole route.

The **undo icmp blackhole unreachable send** command disables the terminal access from sending a Destination Unreachable ICMP packet to an initiator when a tracert packet matches an IPv4 blackhole route.

By default, the terminal access is disabled from sending a Destination Unreachable ICMP packet to an initiator when a tracert packet matches an IPv4 blackhole route.

Format

icmp blackhole unreachable send

undo icmp blackhole unreachable send

Parameters

None

Views

System view

Default Level

2: Configuration level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

If static IPv4 blackhole routes are configured on the terminal access and a user goes offline, only the IPv4 blackhole route corresponding to the user's address segment exists on the terminal access. When a tracert packet matches the IPv4 blackhole route, the terminal access discards the packet. As a result, an initiator cannot detect that the user has gone offline.

After you run the **icmp blackhole unreachable send** command, the terminal access sends a Destination Unreachable ICMP packet to an initiator, notifying the initiator that the user has gone offline if a user goes offline and a tracert packet matches the IPv4 blackhole route.

Pre-configuration Tasks

Static IPv4 blackhole routes have been configured on the terminal access.

Example

Enable the terminal access to send a Destination Unreachable ICMP packet to an initiator when a tracert packet matches an IPv4 blackhole route.

```
<Huawei> system-view
[Huawei] icmp blackhole unreachable send
```

8.7.19 icmp host-unreachable send

Function

The **icmp host-unreachable send** command enables the device to send ICMP host unreachable packets.

The **undo icmp host-unreachable send** command disables the device from sending ICMP host unreachable packets.

By default, the device can send ICMP host unreachable packets.

Format

icmp host-unreachable send

undo icmp host-unreachable send

Parameters

None

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

After you run the **undo icmp host-unreachable send** command, the device does not send ICMP host unreachable packets externally. This prevents the peer device from processing a large number of ICMP packets.

This command needs to be configured on the inbound interface of ICMP packets.

Example

Enable GE1/0/0 to send ICMP host unreachable packets.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] icmp host-unreachable send
```

Related Topics

8.7.8 display icmp statistics

8.7.20 icmp port-unreachable send

Function

The **icmp port-unreachable send** command enables the device to send ICMP port unreachable packets.

The **undo icmp port-unreachable send** command disables the device from sending ICMP port unreachable packets.

By default, the device does not send ICMP port unreachable packets.

Format

icmp port-unreachable send

undo icmp port-unreachable send

Parameters

None

Views

System view and Interface view

Default Level

2: Configuration level

Usage Guidelines

After the function of sending ICMP port unreachable packets is disabled, the device does not send ICMP port unreachable packets. This can reduce the number of ICMP packets on the network and reduce the workload on the peer device.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the device to send ICMP port unreachable packets.

```
<Huawei> system-view
[Huawei] icmp port-unreachable send
```

8.7.21 icmp time-exceed

Function

The **icmp time-exceed** command specifies the format of ICMP Time Exceeded packets.

The **undo icmp time-exceed** command restores the format of ICMP Time Exceeded packets to the default setting.

By default, ICMP Time Exceeded packets carry extension headers in compliant mode and original datagrams are of variable length.

Format

icmp time-exceed { **extension** { **compliant** | **non-compliant** } | **classic** }

undo icmp time-exceed

Parameters

Parameter	Description	Value
extension	Indicates that ICMP Time Exceeded packets carry extension headers.	-
compliant	Indicates that ICMP Time Exceeded packets carry extension headers in compliant mode and original datagrams are of variable length.	-
non-compliant	Indicates that ICMP Time Exceeded packets carry extension headers in non-compliant mode and original datagrams are of fixed length.	-
classic	Indicates that ICMP Time Exceeded packets do not carry extension headers.	-

Views

System view

Default Level

2: Configuration level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

When using the **tracert** command to check the network connectivity, you can run the **icmp time-exceed** command to specify the format of ICMP Time Exceeded packets.

- When the **icmp time-exceed** command carry the parameter **extension compliant**, ICMP Time Exceeded packets carry extension headers in compliant mode and original datagrams are of variable length. ICMP Time Exceeded packets carry as many original datagrams as possible. Lengths of original datagrams carried in ICMP Time Exceeded packets are recorded in ICMP headers.
- When the **icmp time-exceed** command carry the parameter **extension non-compliant**, ICMP Time Exceeded packets carry extension headers in non-compliant mode and original datagrams are of fixed length. If the length of original datagrams is less than 128 bytes, the system automatically fills the length to 128 bytes.
- When the **icmp time-exceed** command carry the parameter **classic**, ICMP Time Exceeded packets do not carry extension headers.

Example

Configure ICMP Time Exceeded packets to carry extension headers in compliant mode.

```
<Huawei> system-view
[Huawei] icmp time-exceed extension compliant
```

Related Topics

21.15.3 tracert

8.7.22 icmp ttl-exceeded drop

Function

The **icmp ttl-exceeded drop** command enables the device to discard the ICMP packets whose TTL values are 1.

The **undo icmp ttl-exceeded drop** command disables the device from discarding the ICMP packets whose TTL values are 1.

By default, the device does not discard the ICMP packets whose TTL values are 1.

Format

icmp ttl-exceeded drop

undo icmp ttl-exceeded drop

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the device receives a large number of IGMP packets, the function enables the device to discard some ICMP packets to reduce the workload on the device.

NOTE

After the function is enabled on the device, the **tracert** command does not take effect.

Example

Enable the device to discard the ICMP packets whose TTL values are 1.

```
<Huawei> system-view
[Huawei] icmp ttl-exceeded drop
```

8.7.23 icmp ttl-exceeded send

Function

The **icmp ttl-exceeded send** command enables an interface to send ICMP Time Exceeded messages.

The **undo icmp ttl-exceeded send** command disables an interface from sending ICMP Time Exceeded messages.

By default, an interface is enabled to send ICMP Time Exceeded messages.

Format

icmp ttl-exceeded send

undo icmp ttl-exceeded send

Parameters

None

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

By default, an interface replies with an ICMP Time Exceeded message after it receives a message with TTL 1. The interface adds its IP address as the source IP address in the ICMP Time Exceeded message, exposing the interface itself to attackers. In addition, after being attacked, the interface replies with numerous ICMP Time Exceeded messages, consuming CPU resources and degrading system performance. To resolve these problems, run the **undo icmp ttl-exceeded send** command to disable the interface from replying with ICMP Time Exceeded messages.

Example

Enable GE1/0/0 from sending ICMP Time Exceeded messages.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] icmp ttl-exceeded send
```

8.7.24 icmp unreachable drop

Function

The **icmp unreachable drop** command enables the function of discarding ICMP destination unreachable packets.

The **undo icmp unreachable drop** command disables the function of discarding the ICMP destination unreachable packets.

By default, the function of discarding ICMP destination unreachable packets is disabled.

Format

icmp unreachable drop

undo icmp unreachable drop

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the function is enabled on the device, the device discards some ICMP packets. This reduces the workload on the device.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the function of discarding ICMP destination unreachable packets.

```
<Huawei> system-view
[Huawei] icmp unreachable drop
```

8.7.25 icmp with-options drop

Function

The **icmp with-options drop** command enables the device to discard ICMP packets that carry options.

The **undo icmp with-options drop** command disables the device from discarding ICMP packets that carry options.

By default, the device does not discard ICMP packets that carry options.

Format

icmp with-options drop

undo icmp with-options drop

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the device receives a large number of ICMP packets, the function enables the device to discard some ICMP packets to reduce the workload on the device.

Example

Enable the device to discard the ICMP packets that carry options.

```
<Huawei> system-view
[Huawei] icmp with-options drop
```

8.7.26 icmp receive

Function

The **icmp receive** command enables the device to receive ICMP messages.

 Copyright © Huawei Technologies Co., Ltd.

The **undo icmp receive** command disables the device from receiving ICMP messages.

By default, the device receives ICMP messages.

Format

icmp { **type** *icmp-type* **code** *icmp-code* | **name** *icmp-name* | **all** } **receive**

undo icmp { **type** *icmp-type* **code** *icmp-code* | **name** *icmp-name* | **all** } **receive**

Parameters

Parameter	Description	Value
type *icmp-type*	Specifies the type number of an ICMP message.	The value is an integer ranging from 0 to 255.
code *icmp-code*	Specifies the code of an ICMP message.	The value is an integer ranging from 0 to 255.
name *icmp-name*	Specifies the name of an ICMP message.	The value is a string of case-insensitive characters, with spaces not supported. The string length ranges from 1 to 32. The value can be any of the following: • echo • echo-reply • fragmentneed-dfset • host-redirect • host-tos-redirect • host-unreachable • information-reply • information-request • net-redirect • net-tos-redirect • net-unreachable • parameter-problem • port-unreachable • protocol-unreachable • reassembly-timeout • source-quench • source-route-failed • timestamp-reply • timestamp-request • ttl-exceeded

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all	Specifies all ICMP packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **undo icmp receive** command can be used to disable the device from receiving ICMP messages for the purpose of improving network performance or enhancing network security.

- On secure networks, the device can normally receive ICMP messages. In the case of heavy traffic on the network, if hosts or ports are frequently unreachable, the device will receive a large number of ICMP packets, which causes heavier traffic burdens over the network and degrades the performance of the device.
- On insecure networks, network attackers often make use of ICMP error messages to probe on the internal structure of the network.

Precautions

If the network status is normal and the device is required to receive ICMP messages, you can run the **icmp receive** command.

After the **undo icmp receive** command is run, the device no longer process ICMP messages of a certain type, causing the host to fail to ping the device.

Example

Disable the device from receiving ICMP messages with the type number being 3 and the code number being 1.

```
<Huawei> system-view
[Huawei] undo icmp type 3 code 1 receive
```

8.7.27 icmp-reply fast

Function

The **icmp-reply fast** command enables the fast ICMP reply function on the device.

The **undo icmp-reply fast** command disables the fast ICMP reply function on the device.

By default, the fast ICMP reply function is enabled on the device.

Copyright © Huawei Technologies Co., Ltd.

Format

icmp-reply fast

undo icmp-reply fast

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the fast ICMP reply function is enabled on the device, the switches fast respond to the ICMP echo request packets whose destination addresses are the addresses of the switches. This improves the device forwarding performance.

NOTE

After the fast ICMP reply function is enabled on the device, the local policy-based routing function does not take effect for ICMP packets. Therefore, if the local policy-based routing function is configured on the device, you are advised to disable the fast ICMP reply function.

Example

Enable the fast ICMP reply function on the device.

```
<Huawei> system-view
[Huawei] icmp-reply fast
```

8.7.28 ip forward-broadcast

Function

The **ip forward-broadcast** command enables an interface to forward directed broadcast packets.

The **undo ip forward-broadcast** command disables an interface from forwarding directed broadcast packets.

By default, an interface is disabled from forwarding directed broadcast packets.

Format

ip forward-broadcast [**acl** *acl-number*]

undo ip forward-broadcast

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
acl *acl-number*	Specifies the number of an ACL.	The value is an integer that ranges from 2000 to 3999. • The number of a basic ACL ranges from 2000 to 2999. • The number of an advanced ACL ranges from 3000 to 3999.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Directed broadcast packets are sent to a specified network. In the destination IP address of a directed broadcast packet, the network number is that of the specified network and the host number is all 1s.

To enable an interface to receive and forward directed broadcast packets destined for its direct network segment, run the **ip forward-broadcast** command. Then the following situations occur:

- The device is allowed to receive directed broadcast packets destined for the interface's direct network segment.
- When the device receives directed broadcast packets destined for this interface's direct network segment through other interfaces, the device forwards these packets through this interface.

Directed broadcast packets can be used by hackers to attack the network system, bringing security risks. However, the device interfaces may need to receive or forward directed broadcast packets in some scenarios. For example, to enable the Wake on LAN function so that directed broadcast packets can be sent to wake up computers on a remote network, enable the interface to receive and forward directed broadcast packets destined for its direct network segment.

The device can also be enabled to receive and forward a certain type of directed broadcast packets based on ACLs. For example, if the basic ACL is used, run the **acl (system view)** and **rule (basic ACL view)** commands to define the directed broadcast packets to be received and forwarded as **permit**, and then run the **ip forward-broadcast** command to bind this ACL.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

By default, the device identifies directed broadcast packets as malformed packets, and intercepts and discards them because the attack defense function of malformed packets is enabled on the device. In this case, the interface on the device cannot forward the directed broadcast packets.

To solve this problem, use either of the following methods:

- Run the **anti-attack abnormal disable** command to disable the attack defense function of malformed packets. However, after this command is configured, other malformed packets will not be intercepted and discarded, which brings certain security risks. Use this command with caution.
- Run the **anti-attack disable** command to disable all attack defense functions. However, after this command is configured, not only malformed packets but also fragmented, tcp-syn, udp-flood, and icmp-flood attack packets will not be intercepted and discarded, which brings certain security risks. Use this command with caution.

You can only configure this command in the VLANIF interface view, Ethernet interface view, GE interface view, XGE interface view, and virtual Ethernet interface view.

This command cannot be used in the VPN scenario, address borrowing scenario, and scenario where the host route and subnet broadcast route conflict because of network segment overlapping.

Example

Enable GE1/0/0 to forward broadcast packets.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip forward-broadcast
```

Related Topics

5.1.9 display ip interface

8.7.29 ip soft-forward enhance enable

Function

The **ip soft-forward enhance enable** command enables the enhanced forwarding function for control packets generated by the device.

The **undo ip soft-forward enhance enable** command disables the enhanced forwarding function for control packets generated by the device.

By default, the enhanced forwarding function is enabled for control packets generated by the device.

Format

ip soft-forward enhance enable

Copyright © Huawei Technologies Co., Ltd.

undo ip soft-forward enhance enable

Parameters

None.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure forwarding policies (such as QoS policies) for data packets to implement differentiated services. In some scenarios, you may need to manage control packets generated by the device to process different control packets. For example, carriers have limited the bandwidth of data packets through QoS policies and also want to limit the bandwidth of control packets. In this situation, QoS policies take effect only for data packets. You can configure the enhanced forwarding function to make QoS policies take effect for control packets. Currently, the enhanced forwarding function is valid only for the control packets generated by the device but not for the control packets forwarded by other devices.

You can run the **ip soft-forward enhance enable** command to enable the enhanced forwarding function for control packets generated by the device.

Follow-up Procedures

After enabling the enhanced forwarding function on the device, you can perform some configurations on the control packets generated by the device. For example, you can configure different QoS policies for different types of packets generated by the device.

Example

Disable the enhanced forwarding function for control packets generated by the device.

```
<Huawei> system-view
[Huawei] undo ip soft-forward enhance enable
```

8.7.30 ip verify source-address

Function

The **ip verify source-address** command enables an interface to check validity of source IP addresses of received packets.

The **undo ip verify source-address** command disables an interface from checking validity of source IP addresses of received packets.

 Copyright © Huawei Technologies Co., Ltd.

By default, an interface does not check validity of source IP addresses of received packets.

Format

ip verify source-address

undo ip verify source-address

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The following IP addresses are illegal source addresses:

- Addresses with all 0s or 1s
- Multicast addresses (class D addresses)
- Class E addresses
- Loopback addresses that are not generated on local hosts (in 127.x.x.x format)
- Broadcast addresses of classes A, B, and C
- Subnet broadcast addresses that are on the same network segment as the address of the inbound interface

The interface only check validity of source IP addresses of the packets that are forwarded to the CPU and does not check validity of source IP addresses of the packets that will be directly forwarded according to the FIB table.

Example

Enable GE1/0/0 to check validity of source addresses of received packets.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip verify source-address
```

Related Topics

3.1.9 display this

 Copyright © Huawei Technologies Co., Ltd.

8.7.31 ip option-virtual-reassembly

Function

The **ip option-virtual-reassembly** command enables virtual fragment reassembly of IP packets with options globally.

The **undo ip option-virtual-reassembly** command disables virtual fragment reassembly of IP packets with options globally.

By default, virtual fragment reassembly of IP packets with options is disabled globally.

Format

ip option-virtual-reassembly

undo ip option-virtual-reassembly

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Oversized IP packets are fragmented during transmission. The intermediate forwarding device forwards the fragmented packets, and the destination device reassembles the fragmented packets after receiving them. If some fragmented packets are discarded during transmission due to bandwidth limitation, the packets cannot be reassembled on the destination device. To solve this problem, you can enable virtual fragment reassembly of IP packets with options globally on the device functioning as the intermediate forwarding device of fragmented packets. The device then checks, sorts, and caches received fragmented packets, and processes the packets uniformly to ensure complete IP packet forwarding or scheduling.

Example

Enable virtual fragment reassembly of IP packets with options globally.

```
<Huawei> system-view
[Huawei] ip option-virtual-reassembly
```

 Copyright © Huawei Technologies Co., Ltd.

8.7.32 ip virtual-reassembly

Function

The **ip virtual-reassembly** command enables virtual fragment reassembly of IP packets.

The **undo ip virtual-reassembly** command disables virtual fragment reassembly of IP packets.

By default, virtual fragment reassembly of IP packets is disabled.

Format

ip virtual-reassembly

undo ip virtual-reassembly

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During network transmission, IP packets are fragmented if they have a long length. The forwarding device forwards the fragmented packets, and the destination device receives the fragmented packets and reassembles them. If some fragmented packets are discarded during transmission due to the bandwidth limitation, the packets cannot be reassembled on the destination device. To solve the problem, you can enable virtual fragment reassembly of IP packets on the device functioning as the intermediate of fragmented packets. After that, the device checks, sorts, and caches the fragmented packets received to ensure complete packet forwarding or scheduling.

Precautions

- If the NAT, firewall, smart application control (SAC), or in-depth security defense functions is configured on the device, virtual fragment reassembly is enabled by default and cannot be disabled. That is, the **undo ip virtual-reassembly** command does not take effect.
- If the upstream device first sends packets whose length is smaller than the interface MTU and then sends packets whose length is equal to the interface MTU after fragmenting packets, you need to run the **ip virtual-reassembly** command to enable the destination device to reassemble fragmented packets.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable virtual fragment reassembly of IP packets.

```
<Huawei> system-view
[Huawei] ip virtual-reassembly
```

8.7.33 load-balance unequal-cost enable

Function

Using the **load-balance unequal-cost enable** command, you can enable the Unequal-Cost Multiple Path (UCMP) function on an interface.

Using the **undo load-balance unequal-cost enable** command, you can disable the UCMP function on an interface.

By default, UCMP is disabled on an interface.

Format

load-balance unequal-cost enable

undo load-balance unequal-cost enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the device, there are multiple equal-cost routes over multiple equal-cost links to a destination. Among the equal-cost links, there are high-speed links and low-speed links. The device evenly load balances traffic over multiple equal-cost links to a single destination regardless of the bandwidth. Consequently, traffic congestion may occur on low-speed links and bandwidth of high-speed links cannot be used efficiently. To solve the preceding problems, configure UCMP so that the equal-cost links carry traffic by bandwidth.

Precautions

This command can only be used on Layer 3 interfaces.

Among all subinterfaces, only the Ethernet sub-interfaces (Dot1q and QinQ termination sub-interfaces) and Eth-trunk sub-interfaces (Dot1q termination sub-interfaces) support configuration of unequal cost multiple path.

 Copyright © Huawei Technologies Co., Ltd.

After enabling or disabling UCMP on an outbound interface of an equal-cost link, run the **shutdown** and **undo shutdown** commands on the outbound interface, or run the **restart** command restarts the interface, to make the configuration take effect.

The equal-cost links carry traffic by bandwidth only when UCMP is enabled on outbound interfaces of all the equal-cost links and FIB entry updating is triggered. If any outbound interface is not enabled with UCMP, the equal-cost links evenly load balance traffic though FIB entry updating is triggered.

On AR120, AR150, AR160, AR200 and AR1200, among the equal-cost links, the bandwidth of any link must be equal to or greater than 1/4 of the total bandwidth; otherwise, the link cannot participate in load balancing traffic by bandwidth.

On AR2200, AR3600 and AR3200, among the equal-cost links, the bandwidth of any link must be equal to or greater than 1/8 of the total bandwidth; otherwise, the link cannot participate in load balancing traffic by bandwidth.

You are advised to configure the bandwidth of each link participating in UCMP to an integral multiple of the minimum bandwidth. If the bandwidth of each link is not configured to an integral multiple of the minimum bandwidth, the system still uses an integral multiple of the minimum bandwidth to process. For example, if the bandwidths of four links participating in UCMP are configured to 2 Kbps, 3 Kbps, 4 Kbps, and 5 Kbps, the final bandwidths of the links are 2 Kbps, 2 Kbps, 4 Kbps, and 4 Kbps.

Before enabling UCMP on a logical interface, run the **load-balance bandwidth** command to manually configure the bandwidth for the logical interface.

Example

Enable UCMP on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] load-balance unequal-cost enable
Warning: The configuration succeeded. Please shutdown/undo shutdown the interfac
e to make changes take effect.
[Huawei-GigabitEthernet1/0/0] shutdown
[Huawei-GigabitEthernet1/0/0] undo shutdown
```

Enable UCMP on Eth-Trunk1.

```
<Huawei> system-view
[Huawei] interface eth-trunk 1
[Huawei-Eth-Trunk1] undo portswitch
[Huawei-Eth-Trunk1] load-balance bandwidth 300000
 Warning: The configuration succeeded. Please shutdown/undo shutdown the interfa
ce to make changes take effect.
[Huawei-Eth-Trunk1] load-balance unequal-cost enable
Warning: The configuration succeeded. Please shutdown/undo shutdown the interfac
e to make changes take effect.
[Huawei-Eth-Trunk1] shutdown
[Huawei-Eth-Trunk1] undo shutdown
```

Related Topics

8.7.34 load-balance bandwidth

 Copyright © Huawei Technologies Co., Ltd.

8.7.34 load-balance bandwidth

Function

The **load-balance bandwidth** command sets the bandwidth of an interface manually.

The **undo load-balance bandwidth** command deletes the manually configured bandwidth of an interface.

For a logical interface, the interface bandwidth is not configured by default; for a physical interface, the actual interface bandwidth is used by default.

Format

load-balance bandwidth *bandwidth*

undo load-balance bandwidth

Parameters

Parameter	Description	Value
bandwidth	Specifies the manually configured bandwidth of an interface.	The value is an integer that ranges from 1 to 10000000, in Kbps.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring the UCMP function, you need to manually set the bandwidth of an interface in the following scenarios:

- Users need to adjust the bandwidth of equal-cost links so that the equal-cost links load balance traffic based on the configured bandwidth.
- The outbound interface of the equal-cost route is a logical interface.

Precautions

This command can only be used on Layer 3 interfaces.

When the manually configured bandwidth of an interface changes or the physical bandwidth corresponding to a logical interface changes, run the **shutdown** and **undo shutdown** commands on the interface to make the new bandwidth take effect.

 Copyright © Huawei Technologies Co., Ltd.

When you manually configure the bandwidth for an interface, the bandwidth ratio of each equal-cost link will change. In UCMP mode, traffic is load balanced by bandwidth. If the bandwidth ratio changes, packets on a link will be lost when the allocated traffic exceeds the physical bandwidth of the link.

You are advised to configure the bandwidth of each link participating in UCMP to an integral multiple of the minimum bandwidth. If the bandwidth of each link is not configured to an integral multiple of the minimum bandwidth, the system still uses an integral multiple of the minimum bandwidth to process. For example, if the bandwidths of four links participating in UCMP are configured to 2 Kbps, 3 Kbps, 4 Kbps, and 5 Kbps, the final bandwidths of the links are 2 Kbps, 2 Kbps, 4 Kbps, and 4 Kbps.

Example

Set the bandwidth of GE1/0/0 to 500000 Kbps.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] load-balance bandwidth 500000
 Warning: The configuration succeeded. Please shutdown/undo shutdown the interfa
ce to make changes take effect.
[Huawei-GigabitEthernet1/0/0] shutdown
[Huawei-GigabitEthernet1/0/0] undo shutdown
```

Related Topics

8.7.33 load-balance unequal-cost enable

8.7.35 reset forward pie counter

Function

The **reset forward pie counter** command clears statistics on packets of the PIE queue.

NOTE

Only the AR169EGW-L, AR169EW, AR161EW, and AR161EW-M1 support this command.

Format

reset forward pie counter

Parameters

None

Views

User view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run the **reset forward pie counter** command to clear statistics on packets of the PIE queue. The cleared statistics cannot be restored. Therefore, confirm your operation before running this command.

Example

Clear PIE queue packet statistics.

```
<Huawei> reset forward pie counter
```

8.7.36 reset ip socket monitor

Function

The **reset ip socket monitor** command clears information in a socket monitor.

Format

reset ip socket monitor [**task-id** *task-id* **socket-id** *socket-id*]

Parameters

Parameter	Description	Value
task-id *task-id*	Clears information about the task with a specified ID in the socket monitor.	The value must be an existing task ID.
socket-id *socket-id*	Clears information about the socket with a specified ID in the socket monitor.	The value must be an existing socket ID.

Views

User view

Default Level

3: Management level

Usage Guidelines

You can specify the task ID and socket ID for deleting information about the socket monitor that meets the filtering condition.

Example

Clear information in a socket monitor.

```
<Huawei> reset ip socket monitor
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

8.7.9 display ip socket

8.7.37 reset ip socket pktsort

Function

The **reset ip socket pktsort** command resets statistics on the dual receive buffer of the socket.

Format

reset ip socket pktsort task-id *task-id* **socket-id** *socket-id*

Parameters

Parameter	Description	Value
task-id *task-id*	Specifies the ID of a task.	The value must be an existing task ID.
socket-id *socket-id*	Specifies the ID of a socket.	The value must be an existing socket ID.

Views

User view

Default Level

3: Management level

Usage Guidelines

This command clears statistics on the dual receive buffer of the socket and restarts the count. Therefore, confirm your action before running the command.

Example

Reset statistics on the dual receive buffer of the socket with the task ID of 2 and the socket ID of 6.

```
<Huawei> reset ip socket pktsort task-id 2 socket-id 6
```

8.7.38 reset ip statistics

Function

The **reset ip statistics** command clears IP traffic statistics on an interface.

Format

reset ip statistics [**interface** *interface-type interface-number*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and ID of an interface. If no optional parameter is specified, all the IP statistics will be deleted.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

To collect IP traffic statistics on an interface in a period of time, you must clear the existing traffic statistics and collect IP statistics after a period of time. Run the **display ip statistics** command to display information.

If no parameter is specified, the command clears IP traffic statistics on all boards.

Example

Clear IP statistics on all interfaces.

```
<Huawei> reset ip statistics
```

Related Topics

5.1.9 display ip interface

8.7.11 display ip statistics

8.7.39 reset rawip statistics

Function

The **reset rawip statistics** command clears RawIP packet statistics.

Format

reset rawip statistics

Parameters

None

Views

User view

Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

The **reset rawip statistics** command clears RawIP packet statistics. Confirm your action before running this command.

Example

Clear RawIP packet statistics.

```
<Huawei> reset rawip statistics
```

Related Topics

8.7.14 display rawip statistics

8.7.40 reset tcp statistics

Function

The **reset tcp statistics** command deletes TCP traffic statistics.

Format

reset tcp statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

The **reset tcp statistics** command deletes TCP traffic statistics. Confirm your action before running this command.

Example

Delete TCP traffic statistics.

```
<Huawei> reset tcp statistics
```

Related Topics

8.7.15 display tcp statistics

 Copyright © Huawei Technologies Co., Ltd.

8.7.41 reset udp statistics

Function

The **reset udp statistics** command deletes UDP traffic statistics.

Format

reset udp statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

The **reset udp statistics** command deletes UDP traffic statistics. Confirm your action before running this command.

Example

Delete UDP traffic statistics.

```
<Huawei> reset udp statistics
```

Related Topics

8.7.17 display udp statistics

8.7.42 set priority dscp

Function

The **set priority dscp** command sets the DSCP priority of control packets generated by the device.

The **undo set priority dscp** command restores the default DSCP priority of control packets generated by the device.

For the default DSCP priorities of control packets generated by the device, see **Table 8-77**.

Format

set priority protocol-type *protocol-type* **dscp** *dscp-value*

Copyright © Huawei Technologies Co., Ltd.

undo set priority protocol-type *protocol-type* **dscp**

set priority acl *acl-number* **dscp** *dscp-value*

undo set priority acl *acl-number*

Parameters

Parameter	Description	Value
protocol-type *protocol-type*	Sets the DSCP priority of control packets based on the protocol type.	The value can be bgp, ftp, icmp, snmp, ssh, **udp**, or telnet.
acl *acl-number*	Sets the DSCP priority of control packets based on the ACL.	The value is an integer that ranges from 3000 to 3999.
dscp *dscp-value*	Specifies the DSCP priority of control packets.	The value is as follows: • The value is an integer that ranges from 0 to 63. • The value can be **ef**, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, or **default**.

Table 8-77 Default DSCP priorities of control packets generated by the device

control Packet	Value
BGP	48
ICMP	0
SNMP	0
SSH	48
Telnet	48
FTP	48

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **ip soft-forward enhance enable** command is executed to enable the enhanced forwarding function of control packets generated by the device, the same QoS policy will be applied to both the control packets and data packets. When the device maps packets based on DSCP priorities, it may send some control packets with low DSCP priorities generated on the device to low-priority queues, such as ICMP and Telnet packets. You can use the **set priority** command to set DSCP priorities of some control packets to prevent them from being sent to low-priority queues.

Precautions

If you run the **set priority** command with the same value of **protocol-type** multiple times, only the latest configuration takes effect.

If the device is configured to set the DSCP priority of control packets based on both the protocol type and ACL, the device sets the DSCP priority of control packets based on the protocol type.

If the device is configured to set the DSCP priority of protocol packets based on ACL rules, a maximum of 16 ACL rules can be configured.

To set DSCP priorities of multiple control packets, run the **set priority** command multiple times.

Example

Set the DSCP priority of Telnet packets to 56.

```
<Huawei> system-view
[Huawei] set priority protocol-type telnet dscp 56
```

Related Topics

8.7.29 ip soft-forward enhance enable

8.7.43 set priority dot1p

Function

The **set priority dot1p** command sets the 802.1p priority of control packets generated by the device.

The **undo set priority dot1p** command restores the default 802.1p priority of control packets generated by the device.

By default, the 802.1p priority of control packets generated by the device is 6.

Copyright © Huawei Technologies Co., Ltd.

Format

set priority dot1p *priority-value*

undo set priority dot1p

Parameters

Parameter	Description	Value
priority-value	Specifies the 802.1p priority of control packets generated by the device.	The value is an integer that ranges from 0 to 7.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The 802.1p priority is determined by the 3-bit priority field contained in a VLAN tag and is used to guarantee QoS in the differentiated services (DiffServ) model.

You can run the **set priority dot1p** command to change the 802.1p priority of control packets generated by the device.

Precautions

If you run the **set priority dot1p** command multiple times, only the latest configuration takes effect.

The **set priority dot1p** command will not take effect on a Layer 2 interface.

Example

Set the 802.1p priority of control packets generated by the device to 5.

```
<Huawei> system-view
[Huawei] set priority dot1p 5
```

8.7.44 set workmode lan-card l3centralize

Function

The **set workmode lan-card l3centralize** command disables the routing and forwarding function on 8FE1GE and 24GE cards.

 Copyright © Huawei Technologies Co., Ltd.

The **undo set workmode lan-card l3centralize** command enables the routing and forwarding function on 8FE1GE and 24GE cards.

By default, the routing and forwarding function is enabled on 8FE1GE and 24GE cards.

Format

set workmode lan-card l3centralize

undo set workmode lan-card l3centralize

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Configuring ACLs on 8FE1GE and 24GE cards is complex, and ACL-based traffic policy and URPF cannot be configured on 8FE1GE and 24GE cards. This restricts the use of ACLs. When the routing and forwarding function is disabled on 8FE1GE and 24GE cards, you can redirect the packets received on 8FE1GE and 24GE cards to the sub-core CPU for packet forwarding. In this situation, you can configure ACL-based traffic policies and URPF and simplify the ACL configuration.

Configuration Impact

- After the **set workmode lan-card l3centralize** command is used, an interface can only be manually added to a voice VLAN.
- After the **set workmode lan-card l3centralize** command is used, protocol packets with source or destination MAC addresses as blackhole MAC addresses will not be discarded.
- After the **set workmode lan-card l3centralize** command is used, the device CPU usage increases.

NOTE

Only AR1200, AR2200, AR3600 and AR3200 support this command.

Example

Disable the routing and forwarding function on 8FE1GE and 24GE cards.

```
<Huawei&gt; system-view
[Huawei] set workmode lan-card l3centralize
```

 Copyright © Huawei Technologies Co., Ltd.

8.7.45 tcp adjust-mss

Function

The **tcp adjust-mss** command sets the maximum segment size (MSS) of TCP packets on an interface.

The **undo tcp adjust-mss** command deletes the configured MSS of TCP packets.

By default, the MSS of TCP packets is not set on the interface.

Format

tcp adjust-mss *value*

undo tcp adjust-mss

Parameters

Parameter	Description	Value
value	Specifies the MSS of TCP packets on an interface.	The value is an integer that ranges from 128 to 2048, in bytes.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The MSS of TCP packets is an option defined in TCP. It refers to the maximum length of a TCP packet segment that can be received by the peer device. When establishing the TCP connection, the local and peer ends negotiate the MSS value to determine the maximum data length of TCP packets. If the length of a TCP packet sent by the peer device exceeds the negotiated MSS, the TCP packet is fragmented.

Precautions

- To ensure that TCP packets are not fragmented, pay attention to the relationship between the MSS and MTU during configuration. MTU is an option used to identify whether IP packets need to be fragmented. If the size of an IP packet sent by the peer device exceeds the MTU, the IP packet is fragmented. To ensure that the packet transmission is not affected, the MSS value plus the header lengths (such as the TCP header and IP header) does not exceed the MTU value. For example, the default MTU value of an

Copyright © Huawei Technologies Co., Ltd.

Ethernet interface is 1500 bytes. To ensure that packets are not fragmented, the MSS value can be set to 1460 bytes. The formula is as follows: Default MTU value (1500 bytes) – Minimum length of the TCP header (20 bytes) – Minimum length of the IP header (20 bytes). The recommended MSS value is 1200 bytes.

- The **tcp adjust-mss** command does not only take effect for the router functioning as the client or server used for TCP connections. When another device functions as the client to perform MSS negotiation through the router, the negotiation result is modified based on the MSS configured on the router. In addition, the MSS value is changed to the value configured using the **tcp adjust-mss** command only when the MSS value received by the router is larger than the value configured using the **tcp adjust-mss** command executed on the router.
- If you run the **tcp adjust-mss** multiple times in the same interface view, only the latest configuration takes effect.

Example

Set the MSS of TCP packets on GE1/0/0 to 1200 bytes.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] tcp adjust-mss 1200
```

Related Topics

5.2.27 mtu (Ethernet interface view)

8.7.49 tcp timer syn-timeout

8.7.50 tcp window

8.7.46 tcp min-mss

Function

The **tcp min-mss** command sets the minimum value of maximum segment size (MSS) for a TCP connection.

The **undo tcp min-mss** command restores the default minimum value of the MSS for a TCP connection.

The default minimum MSS value for a TCP connection is 216 bytes.

Format

tcp min-mss *mss-value*

undo tcp min-mss

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
mss-value	Specifies the minimum MSS value for a TCP connection.	The value ranges from 32 byte to 1500 bytes. By default, the value is 216 bytes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To establish a TCP connection, the MSS value is negotiated, which indicates the maximum length of packets that the local device can receive. The TCP client on a network may send a request packet for establishing a TCP connection carrying a small MSS value. For example, the MSS value is 1. After the TCP server receives the request packet carrying the MSS value, the TCP connection is established. The TCP client then may send large numbers of requests to the server by an application, causing the TCP server to generate large numbers of reply packets. This may burden the TCP server or network, causing denial of service (DoS) attacks. To resolve this problem, run the **tcp min-mss** command to set the minimum MSS value for a TCP connection. This configuration prevents a server from receiving packets carrying a small MSS value.

Precautions

If the **tcp min-mss** command is run more than once in the same view, the latest configuration overrides the previous one.

Configure the parameters under the guidance of the technical personnel.

Example

Set the minimum MSS value for a TCP connection to 512 bytes.

```
<Huawei> system-view
[Huawei] tcp min-mss 512
```

Related Topics

8.7.50 tcp window

Copyright © Huawei Technologies Co., Ltd.

8.7.47 tcp timer fin-timeout

Function

The **tcp timer fin-timeout** command configures the value of the TCP FIN-Wait timer.

The **undo tcp timer fin-timeout** command restores the default value of the TCP FIN-Wait timer.

By default, the value of the TCP FIN-Wait timer is 675s.

Format

tcp timer fin-timeout *interval*

undo tcp timer fin-timeout

Parameters

Parameter	Description	Value
interval	Specifies the value of the TCP FIN-Wait timer.	The value is an integer that ranges from 76 to 3600, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a TCP connection changes from FIN_WATI_1 to FIN_WAIT_2, the TCP FIN-Wait timer is started. If no response packet is received after the TCP FIN-Wait timer expires, the TCP connection is closed.

If you run this command in the same view for multiple times, only the last configuration takes effect.

You are advised to configure this parameter under the supervision of technical support personnel.

Example

Set the value of the TCP FIN-Wait timer to 400s.

```
<Huawei> system-view
[Huawei] tcp timer fin-timeout 400
```

Related Topics

8.7.49 tcp timer syn-timeout

Copyright © Huawei Technologies Co., Ltd.

8.7.50 tcp window

8.7.48 tcp timer pathmtu-age

Function

The **tcp timer pathmtu-age** command sets the aging time for a TCP PMTU.

The **undo tcp timer pathmtu-age** command restores the aging time for a TCP PMTU to the default value.

By default, the aging time of the PMTU is 0 minutes, that is, the PMTU never ages.

Format

tcp timer pathmtu-age *age-time*

undo tcp timer pathmtu-age

Parameters

Parameter	Description	Value
age-time	Specifies the aging time for a TCP PMTU.	The value is an integer that ranges from 10 to 100, in minutes. The default value is 0 minutes, which is recommended.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When hosts on the same network communicate with each other, the MTU of the network is important for the hosts. When hosts communicate with each other across multiple networks, it is important to determine the minimum MTU on the network path because the MTUs of the link layers on different networks are different. The minimum MTU on the network path is called the path MTU (PMTU).

When hosts on the network communicate with each other, the interface MTU on the communication path may change. This may cause the following problems:

- If the interface MTU changes to a smaller value, the system refragments the data packets to be sent and learn a new PMTU. This affects data transmission efficiency and network performance.

 Copyright © Huawei Technologies Co., Ltd.

- If the interface MTU changes to a value greater than the PMTU, the interface MTU will be too big for transmitting the fragmented packets. This also affects data transmission efficiency and network performance.

To prevent the preceding problems, run the **tcp timer pathmtu-age** command to set the aging time for a PMTU. After the PMTU ages, the device sends data packets based on the MTU of the outbound interface to detect the PMTU change.

Configuration Impact

The **tcp timer pathmtu-age** command changes only the aging time of dynamic PMTUs. It is not applicable to static PMTUs because static PMTUs cannot age.

Precautions

You need to set a PMTU based on network stability. The default PMTU is recommended. That is, a PMTU does not age.

- If the aging time of a PMTU is set too longer, the PMTU may not be updated in time. This will affect network performance.
- If the aging time of a PMTU is set too short, data transmission efficiency on the network will be affected.

Example

Set the aging time of a TCP PMTU to 50 minutes.

```
<Huawei> system view
[Huawei] tcp timer pathmtu-age 50
```

8.7.49 tcp timer syn-timeout

Function

The **tcp timer syn-timeout** command configures the value of the TCP SYN-Wait timer.

The **undo tcp timer syn-timeout** command restores the default value of the TCP SYN-Wait timer.

By default, the value of the TCP SYN-Wait timer is 75s.

Format

tcp timer syn-timeout *interval*

undo tcp timer syn-timeout

Parameters

Parameter	Description	Value
interval	Specifies the value of the TCP SYN-Wait timer.	The value is an integer ranging from 2 to 600, in seconds. The default value is 75s.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When an SYN packet is sent, the TCP SYN-Wait timer is started. If no response packet is received after the TCP SYN-Wait timer expires, the TCP connection is closed.

If you run this command in the same view for multiple times, only the last configuration takes effect.

You are advised to configure this parameter under the supervision of technical support personnel.

Example

Set the value of the TCP SYN-Wait timer to 100s.

```
<Huawei> system-view
[Huawei] tcp timer syn-timeout 100
```

Related Topics

8.7.47 tcp timer fin-timeout

8.7.50 tcp window

8.7.50 tcp window

Function

The **tcp window** command configures the size of the receive or send buffer of a connection-oriented socket.

The **undo tcp window** command restores the default size of the receive or send buffer of a connection-oriented socket.

By default, the size of the receive or send buffer of a connection-oriented socket is 8k bytes.

Format

tcp window *window-size*

undo tcp window

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
window-size	Specifies the size of the receive or send buffer of a connection-oriented socket.	The value is an integer that ranges from 1 to 32, in k bytes. The default value is 8k bytes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If you run this command in the same view for multiple times, only the last configuration takes effect.

You are advised to configure this parameter under the supervision of technical support personnel.

Example

Set the size of the receive or send buffer of a connection-oriented socket to 3K bytes.

```
<Huawei> system-view
[Huawei] tcp window 3
```

Related Topics

8.7.47 tcp timer fin-timeout

8.7.49 tcp timer syn-timeout

8.8 Basic IPv6 Configuration Commands

8.8.1 control-packet-ipv6 output car bypass

Function

The **control-packet-ipv6 output car bypass** command configures the IPv6 control packets generated by the device not to support traffic policing function.

The **undo control-packet-ipv6 output car bypass** command configures the IPv6 control packets generated by the device to support traffic policing function.

By default, IPv6 control packets generated by the device do not support traffic policing function.

Copyright © Huawei Technologies Co., Ltd.

Format

control-packet-ipv6 { **bgp4plus** | **icmpv6** | **dns6** | **snmp** | **ssh** | **telnet** | **udp** [*ip_address port*] }* **output car bypass**

control-packet-ipv6 all output car bypass

undo control-packet-ipv6 { **bgp4plus** | **icmpv6** | **dns6** | **snmp** | **ssh** | **telnet** | **udp** [*ip_address port*] }* **output car bypass**

undo control-packet-ipv6 all output car bypass

Parameters

Parameter	Description	Value
bgp4plus	Indicates BGP4+ control packets.	-
icmpv6	Indicates ICMPv6 control packets.	-
dns6	Indicates IPv6 DNS control packets.	-
snmp	Indicates IPv6 SNMP control packets.	-
ssh	Indicates IPv6 SSH control packets.	-
telnet	Indicates IPv6 TELNET control packets.	-
udp	Indicates IPv6 UDP control packets.	-
ip_address	Indicates IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
port	Indicates the port.	The value is an integer that ranges from 0 to 65535.
all	Indicates all IPv6 control packets.	-

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the enhanced forwarding function is enabled for IPv6 control packets generated by the device, you can run the **undo control-packet-ipv6 output car bypass** command to configures IPv6 control packets generated by the device to support traffic policing function to apply QoS policies to different control packets.

Follow-up Procedures

After IPv6 control packets generated by the device are configured to support traffic policing function, configure QoS policies to process different control packets. For details about traffic policing configuration, see Configuring Traffic Policing in *Huawei AR Series Access Routers Configuration Guide-QoS*.

Precautions

- Before configuring IPv6 control packets generated by the device to support traffic policing function, enable the enhanced forwarding function for IPv6 control packets generated by the device (using the **8.8.57 ipv6 soft-forward enhance enable** command). After IPv6 control packets generated by the device are configured to support traffic policing function, control packets may be discarded, affecting user services.
- When **bgp4plus**, **dns6**, **icmpv6**, **snmp**, **ssh**, **telnet** and **udp** are specified in the **undo control-packet-ipv6 car bypass** commands, the device generates a configuration file of the **undo control-packet-ipv6 all output car bypass** command. If the **control-packet-ipv6 output car bypass** command is then executed to configure a specified type of IPv6 control packets generated by the device not to support traffic policing function, the device does not generate the configuration file of the **undo control-packet-ipv6 all output car bypass** command but generates the configuration files of the control packets that are configured to support traffic policing function. For example, if BGP4+ packets, IPv6 DNS packets, ICMPv6 packets, IPv6 SNMP packets, IPv6 SSH packets and IPv6 UDP packets generated by the device are configured not to support traffic policing function, the device generates the configuration files of the **undo control-packet-ipv6 telnet output car bypass** commands.

Example

Configure BGP4+ packets generated by the device to support traffic policing function.

```
<Huawei> system-view
[Huawei] undo control-packet-ipv6 bgp4plus output car bypass
```

Related Topics

8.8.57 ipv6 soft-forward enhance enable

Copyright © Huawei Technologies Co., Ltd.

8.8.2 control-packet-ipv6 output filter bypass

Function

The **control-packet-ipv6 output filter bypass** command configures the device not to discard generated IPv6 control packets when the traffic policy and ACL-based simplified traffic policy contain the deny action.

The **undo control-packet-ipv6 output filter bypass** command configures the device to discard generated IPv6 control packets when the traffic policy and ACL-based simplified traffic policy contain the deny action.

By default, the device does not discard generated IPv6 control packets when the traffic policy and ACL-based simplified traffic policy contain the deny action.

Format

control-packet-ipv6 { **bgp4plus** | **icmpv6** | **dns6** | **snmp** | **ssh** | **telnet** | **udp** [*ip_address port*] }* **output filter bypass**

control-packet-ipv6 all output filter bypass

undo control-packet-ipv6 { **bgp4plus** | **icmpv6** | **dns6** | **snmp** | **ssh** | **telnet** | **udp** [*ip_address port*] }* **output filter bypass**

undo control-packet-ipv6 all output filter bypass

Parameters

Parameter	Description	Value
bgp4plus	Indicates BGP4+ control packets.	-
dns6	Indicates IPv6 DNS control packets.	-
icmpv6	Indicates ICMPv6 control packets.	-
snmp	Indicates IPv6 SNMP control packets.	-
ssh	Indicates IPv6 SSH control packets.	-
telnet	Indicates IPv6 TELNET control packets.	-
udp	Indicates IPv6 UDP control packets.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ip_address	Indicates IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
port	Indicates the port.	The value is an integer that ranges from 0 to 65535.
all	Indicates all IPv6 control packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the enhanced forwarding function is enabled for IPv6 control packets generated by the device, the device does not discard the control packets when the traffic policy and ACL-based simplified traffic policy contain the deny action. After the **undo control-packet-ipv6 output filter bypass** command is executed, the device is configured to discard generated IPv6 control packets when the traffic policy and ACL-based simplified traffic policy contain the deny action and apply QoS policy to the control packets to meet different service requirements.

Follow-up Procedures

The packet filter action in the traffic policy or ACL-based simplified traffic policy has been set to deny.

Precautions

- Before configuring the device to discard generated IPv6 control packets when the traffic policy and ACL-based simplified traffic policy contain the deny action, enable the enhanced forwarding function for IPv6 control packets generated by the device (using the **8.8.57 ipv6 soft-forward enhance enable command**). **After the device is configured to discard generated IPv6 control packets when the traffic policy and ACL-based simplified traffic policy contain the deny action, user services may be affected.**
- When **bgp4plus**, **dns6**, **icmpv6**, **snmp**, **ssh**, **udp** and **telnet** are specified in the **undo control-packet-ipv6 output filter bypass** commands, the device

Copyright © Huawei Technologies Co., Ltd.

generates a configuration file of the **undo control-packet-ipv6 all output filter bypass** command. If the **control-packet-ipv6 output filter bypass** command is then executed to configure the device not to discard a specified type of control packets, the device does not generate the configuration file of the **undo control-packet-ipv6 all output filter bypass** command but generates the configuration files of the control packets that the device is configured to discard. For example, if the device is configured not to discard BGP4+ packets, IPv6 DNS packets, ICMPv6 packets, IPv6 SNMP packets and IPv6 SSH packets, the device generates the configuration files of the **undo control-packet-ipv6 telnet output filter bypass** commands.

Example

Configure the device to discard generated BGP4+ packets when the traffic policy and ACL-based simplified traffic policy contain the deny action.

```
<Huawei> system-view
[Huawei] undo control-packet-ipv6 bgp4plus output filter bypass
```

Related Topics

8.8.57 ipv6 soft-forward enhance enable

8.8.3 control-packet-ipv6 output queue bypass

Function

The **control-packet-ipv6 output queue bypass** command configures the IPv6 control packets generated by the device not to support QoS queue functions (such as traffic shaping, congestion management, and congestion avoidance).

The **undo control-packet-ipv6 output queue bypass** command configures the IPv6 control packets generated by the device to support QoS queue functions (such as traffic shaping, congestion management, and congestion avoidance).

By default, IPv6 control packets generated by the device do not support QoS queue functions.

Format

control-packet-ipv6 { **bgp4plus** | **icmpv6** | **dns6** | **snmp** | **ssh** | **telnet** | **udp** [*ip_address port*] }* **output queue bypass**

control-packet-ipv6 all output queue bypass

undo control-packet-ipv6 { **bgp4plus** | **icmpv6** | **dns6** | **snmp** | **ssh** | **telnet** | **udp** [*ip_address port*] }* **output queue bypass**

undo control-packet-ipv6 all output queue bypass

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
bgp4plus	Indicates BGP4+ control packets.	-
icmpv6	Indicates ICMPv6 control packets.	-
dns6	Indicates IPv6 DNS control packets.	-
snmp	Indicates IPv6 SNMP control packets.	-
ssh	Indicates IPv6 SSH control packets.	-
telnet	Indicates IPv6 TELNET control packets.	-
udp	Indicates IPv6 UDP control packets.	-
ip_address	Indicates IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
port	Indicates the port.	The value is an integer that ranges from 0 to 65535.
all	Indicates all IPv6 control packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the enhanced forwarding function is enabled for IPv6 control packets generated by the device, you can run the **undo control-packet-ipv6 output queue bypass** command to configures IPv6 control packets generated by the

 Copyright © Huawei Technologies Co., Ltd.

device to support QoS queue functions (such as traffic shaping, congestion management, and congestion avoidance) to apply QoS policies to different control packets.

Follow-up Procedures

After IPv6 control packets generated by the device are configured to support QoS queue functions, configure QoS policies to process different control packets.

Precautions

- Before configuring IPv6 control packets generated by the device to support QoS queue functions, enable the enhanced forwarding function for IPv6 control packets generated by the device (using the **8.8.57 ipv6 soft-forward enhance enable** command). After IPv6 control packets generated by the device are configured to support QoS queue functions, control packets may be discarded, affecting user services.
- When **bgp4plus**, **dns6**, **icmpv6**, **snmp**, **ssh**, **udp**, and **telnet** are specified in the **undo control-packet-ipv6 output queue bypass** commands, the device generates a configuration file of the **undo control-packet-ipv6 all output queue bypass** command. If the **control-packet-ipv6 output queue bypass** command is then executed to configure a specified type of control packets generated by the device not to support QoS queue functions, the device does not generate the configuration file of the **undo control-packet-ipv6 all output queue bypass** command but generates the configuration files of the control packets that are configured to support QoS queue functions. For example, if BGP4+ packets, IPv6 DNS packets, ICMPv6 packets, IPv6 SNMP packets, and IPv6 SSH packets generated by the device are configured not to support QoS queue functions, the device generates the configuration files of the **undo control-packet-ipv6 telnet output queue bypass** commands.

Example

Configure BGP4+ packets generated by the device to support QoS queue functions.

```
<Huawei> system-view
[Huawei] undo control-packet-ipv6 bgp4plus output queue bypass
```

Related Topics

8.8.57 ipv6 soft-forward enhance enable

8.8.4 display default-parameter tcp6

Function

The **display default-parameter tcp6** command displays the default values of all configurable parameters on the TCP6 module.

Format

display default-parameter tcp6

Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the default values of all configurable parameters on the TCP6 module.

```
<Huawei> display default-parameter tcp6
---------------------------------
 SYN Timeout Value(sec) : 75
 FIN Timeout Value(sec) : 600
 Window Size(KBytes)    : 8
---------------------------------
```

Table 8-78 Description of the display default-parameter tcp6 command output

Item	Description
SYN Timeout Value(sec)	TCP SYN-WAIT timer value. To configure this parameter, run the **tcp ipv6 timer syn-timeout** command.
FIN Timeout Value(sec)	TCP FIN-WAIT timer value. To configure this parameter, run the **tcp ipv6 timer fin-timeout** command.
Window Size(KBytes)	TCP6 slide window size. To configure this parameter, run the **tcp ipv6 window** command.

Related Topics

8.8.73 tcp ipv6 timer syn-timeout

8.8.72 tcp ipv6 timer fin-timeout

8.8.74 tcp ipv6 window

Copyright © Huawei Technologies Co., Ltd.

8.8.5 display icmpv6 statistics

Function

The **display icmpv6 statistics** command displays ICMPv6 traffic statistics.

Format

display icmpv6 statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays ICMPv6 traffic statistics on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If no interface is specified, ICMPv6 traffic statistics on all interfaces are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display icmpv6 statistics** command to view ICMPv6 packet statistics, including statistics about received and sent ICMPv6 error packets and statistics about four types of ICMPv6 packets (RS, RA, NS, and NA packets) used in the neighbor discovery mechanism.

When you ping an IPv6 address from a device, run the **display icmpv6 statistics** command on the device to check whether the total number of sent and received packets is correct.

Precautions

The total number of packets received by the device includes the number of packets forwarded, number of packets delivered to upper-layer network devices, and number of packets discarded.

Example

Display ICMPv6 traffic statistics on the device.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display icmpv6 statistics
ICMPv6 protocol:
  Sent packets:
    Total              : 0
    Unreached          : 0             Prohibited         : 0
    Hop count exceeded : 0             Parameter problem  : 0
    Too big            : 0             Echoed             : 0
    Echo replied       : 0             Router solicit     : 0
    Router advert      : 0             Neighbor solicit   : 2
    Neighbor advert    : 0             Redirected         : 0
    Rate limited       : 0
  Received packets:
    Total              : 0             Format error       : 0
    Checksum error     : 0             Too short          : 0
    Bad code           : 0             Bad length         : 0
    Unknown info type  : 0             Unknown error type : 0
    Unreached          : 0             Prohibited         : 0
    Hop count exceeded : 0             Parameter problem  : 0
    Too big            : 0             Echoed             : 0
    Echo replied       : 0             Router solicit     : 0
    Router advert      : 0             Neighbor solicit   : 0
    Neighbor advert    : 0             Redirected         : 0
    Rate limited       : 0
```

Table 8-79 Description of the display icmpv6 statistics command output

Item	Description
ICMPv6 protocol	ICMPv6 packet statistics.
Sent packets	Statistics about sent ICMPv6 packets.
Total	Total number of sent packets.
Unreached	Total number of sent ICMPv6 Destination Unreachable packets.
Prohibited	Total number of sent ICMPv6 Administratively Prohibited Unreachable packets.
Hop count exceeded	Total number of sent ICMPv6 packets whose hops exceed the limit.
Parameter problem	Total number of sent ICMPv6 Parameter Problem packets.
Too big	Total number of sent ICMPv6 Packet Too Big packets.
Echoed	Total number of sent ICMPv6 Echo Request packets.
Echo replied	Total number of sent ICMPv6 Echo Reply packets.
Router solicit	Total number of sent Router Solicitation (RS) packets.
Router advert	Total number of sent Router Advertisement (RA) packets.
Neighbor solicit	Total number of sent Neighbor Solicitation (NS) packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Neighbor advert	Total number of sent Neighbor Advertisement (NA) packets.
Redirected	Total number of sent ICMPv6 Redirect packets.
Rate limited	Total number of ICMPv6 packets that fail to be sent because of the rate limit.
Received packets	Statistics about received ICMPv6 packets.
Total	Total number of received packets.
Format error	Total number of received ICMPv6 packets with format errors.
Checksum error	Total number of received ICMPv6 packets with checksum errors.
Too short	Total number of received ICMPv6 packets that are too short.
Bad code	Total number of received ICMPv6 packets with code errors.
Bad length	Total number of received ICMPv6 packets with packet length errors.
Unknown info type	Total number of received ICMPv6 packets with an unknown information type.
Unknown error type	Total number of received ICMPv6 packets with an unknown error type.
Unreached	Total number of received ICMPv6 Destination Unreachable packets.
Prohibited	Total number of received ICMPv6 Administratively Prohibited Unreachable packets.
Hop count exceeded	Total number of received ICMPv6 packets whose hops exceed the limit.
Parameter problem	Total number of received ICMPv6 Parameter Problem packets.
Too big	Total number of received ICMPv6 packets that are oversized.
Echoed	Total number of received ICMPv6 Echo Request packets.
Echo replied	Total number of received ICMPv6 Echo Reply packets.
Router solicit	Total number of received RS packets.
Router advert	Total number of received RA packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Neighbor solicit	Total number of received NS packets.
Neighbor advert	Total number of received NA packets.
Redirected	Total number of received ICMPv6 Redirect packets.
Rate limited	Total number of ICMPv6 packets that fail to be received because of the rate limit.

Related Topics

8.8.13 display ipv6 statistics

8.8.6 display ipv6 address-policy

Function

The **display ipv6 address-policy** command displays address selection policy entries.

Format

display ipv6 address-policy [**vpn-instance** *vpn-instance-name*] { **all** | *ipv6-address prefix-length* }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays address selection policy entries of a specified VPN instance.	The value must be an existing VPN instance.
all	Displays all address selection policy entries.	-
ipv6-address	Specifies an IPv6 address prefix.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
prefix-length	Specifies the prefix length of an IPv6 address.	The value is an integer that ranges from 0 to 128.

Views

All views

Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When using this command, pay attention to the following points:

- If the **all** parameter is specified, all address selection policy entries including the default ones are displayed.
- If the *ipv6-address prefix-length* parameter is specified, address selection policy entries of the specific prefix are displayed.

Precautions

If no address selection policy entry is configured, this command displays only the default address selection policy entries. These entries are prefixed with ::1, ::, 2002::, FC00::, and ::FFFF:0.0.0.0.

Example

Display address selection policy entries of VPN instance R1_VPN6.

```
<Huawei> display ipv6 address-policy vpn-instance R1_VPN6 all
Policy Table :
            Total:5
------------------------------------------------------------------------------
Prefix     : ::                                PrefixLength  : 0
Precedence : 40                                     Label        : 1
Default    : Yes

Prefix     : ::1                               PrefixLength  : 128
Precedence : 50                                     Label        : 0
Default    : Yes

Prefix     : ::FFFF:0.0.0.0                      PrefixLength  : 96
Precedence : 10                                     Label        : 4
Default    : Yes

Prefix     : 2002::                            PrefixLength  : 16
Precedence : 30                                     Label        : 2
Default    : Yes

Prefix     : FC00::                            PrefixLength  : 7
Precedence : 20                                     Label        : 3
Default    : Yes
------------------------------------------------------------------------------
```

Table 8-80 Description of the display ipv6 address-policy command output

Item	Description
Policy Table	Address selection policy entries.
Total	Number of address selection policy entries.
Prefix	IPv6 address prefix.
PrefixLength	Length of the IPv6 address prefix.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Precedence	Priority of an IPv6 address when the address is the destination address.
Label	Priority of an IPv6 address when the address is the source address.
Default	Whether an address selection policy entry is the default policy entry: • Yes: The policy entry is the default policy entry. • No: The policy entry is not the default policy entry.

Related Topics

8.8.27 ipv6 address-policy

8.8.7 display ipv6 attack-source overlapping-fragment

Function

The **display ipv6 attack-source overlapping-fragment** displays source information about overlapping fragment attacks.

Format

display ipv6 attack-source overlapping-fragment

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When suffering from overlapping fragment attacks, you can use this command to view source information about attack packets. Source information includes the source and destination IP addresses of the packets, interface receiving the packets, source VLAN, source CE VLAN, and VPN to which the packets belongs. You can take proper actions on the attack source.

Example

Display source information about overlapping fragment attacks.

Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display ipv6 attack-source overlapping-fragment
Attack-source overlapping fragment table:

------------------------------------------------------------------------------
 Source IP          : FC00::1
 Destination IP     : FC00::2
 Interface name     : Eth0/0/0
 VPN name           :
 VLAN               : 0                          CEVLAN: 0
 Attacked time      : 2011-09-29 01:01:28
------------------------------------------------------------------------------

Total: 1
```

Table 8-81 Description of the display ipv6 attack-source overlapping-fragment command output

Item	Description
Source IP	Source IPv6 address of an overlapping fragment attack packet.
Destination IP	Destination IPv6 address of the overlapping fragment attack packet.
Interface name	Interface that receives the overlapping fragment attack packet.
VPN name	Name of the VPN to which the overlapping fragment attack packet belongs.
VLAN	VLAN to which the overlapping fragment attack packet belongs.
CEVLAN	CE VLAN to which the overlapping fragment attack packet belongs.
Attacked time	Duration of the overlapping fragment attack.
Total	Number of pieces of source information about overlapping fragment attacks.

Related Topics

8.8.59 reset ipv6 attack-source overlapping-fragment

8.8.8 display ipv6 interface

Function

The **display ipv6 interface** command displays IPv6 information on an interface.

Format

display ipv6 interface [*interface-type interface-number* | **brief**]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-type interface-number	Displays IPv6 information on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If no interface is specified, IPv6 information on all interfaces configured with IPv6 addresses is displayed.	-
brief	Displays brief information about the interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before running this command, ensure that the interface is configured with an IPv6 address. If no IPv6 address is assigned to the interface, no interface information is displayed.

Example

Display IPv6 information on GE1/0/0.

```
<Huawei> display ipv6 interface gigabitethernet 1/0/0
GigabitEthernet1/0/0 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::200:1FF:FE04:5D00
  Global unicast address(es):
    FC00::1, subnet is FC00::/64
  Joined group address(es):
    FF02::1:FF00:1
    FF02::1:FF04:5D00
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND stale time is 1200 seconds
  Hosts use stateless autoconfig for addresses
```

 Copyright © Huawei Technologies Co., Ltd.

Table 8-82 Description of the display ipv6 interface command output

Item	Description
link-local address	Link-local address configured on the interface. To configure a link-local address for an interface, run the **ipv6 address link-local** command.
Global unicast address(es)	Global unicast address configured on the interface. To configure a global unicast address for an interface, run the **ipv6 address** command.
Joined group address(es)	Addresses of all multicast groups that the interface joins.
MTU	MTU of the interface.
ND DAD is enabled	NS packets are sent when the system performs Duplicate Address Detection (DAD).
number of DAD attempts	Number of times duplicate address detection is performed.
ND reachable time	Neighbor reachable time.
ND retransmit interval	Retransmission interval.
Hosts use stateless autoconfig for addresses	Hosts obtain IPv6 addresses using stateless autoconfiguration.
ND stale time	Time period for the neighbor to keep the STALE state.

Related Topics

8.8.21 ipv6 address

8.8.9 display ipv6 interface tunnel

Function

The **display ipv6 interface tunnel** command displays IPv6 information on a tunnel interface.

Format

display ipv6 interface tunnel *interface-number*

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-number	Displays the tunnel interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display IPv6 information on Tunnel0/0/1.

```
<Huawei> display ipv6 interface tunnel 0/0/1
Tunnel0/0/1 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::201:102 [TENTATIVE]
  Global unicast address(es):
    ::2.1.1.2, subnet is ::/96 [TENTATIVE]
  Joined group address(es):
    FF02::1:FF01:102
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
```

Table 8-83 Description of the display ipv6 interface tunnel command output

Item	Description
Tunnel0/0/1 current state	Current status of the tunnel interface: • UP: enabled • DOWN: disabled When working properly, an IPv6 over IPv4 tunnel is in Up state.
IPv6 protocol current state	Current status of the link layer protocol: • UP: enabled • DOWN: disabled When working properly, an IPv6 over IPv4 tunnel is in Up state.
IPv6 is enabled	IPv6 is enabled.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
link-local address	Link-local address. To configure a link-local address, run the **ipv6 address link-local** command.
Global unicast address(es)	IPv6 global unicast address. To configure an IPv6 global unicast address, run the **ipv6 address** command.
Joined group address(es)	Addresses of multicast groups that the interface joins.
MTU	MTU of the interface.
ND reachable time	Interval for ND unreachability detection.
ND retransmit interval	Interval for retransmitting ND packets.
Hosts use stateless autoconfig for addresses	Hosts obtain IPv6 addresses through stateless address autoconfiguration.

Related Topics

8.8.8 display ipv6 interface

8.8.10 display ipv6 neighbors

Function

The **display ipv6 neighbors** command displays information about neighbor entries.

Format

display ipv6 neighbors [*ipv6-address* | [**vid** *vid*] *interface-type interface-number* | **vpn-instance** *vpn-instance-name*]

display ipv6 neighbors *interface-type interface-number* [**vid** *vid* [**cevid** *cevid*]]

Parameters

Parameter	Description	Value
ipv6-address	Displays neighbor entries of a specified IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
vid *vid*	Displays neighbor entries of a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Displays neighbor entries on a specified interface.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays neighbor entries of a specified VPN instance.	The value must be an existing VPN instance.
cevid *cevid*	Specifies the inner VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ipv6 neighbors** command displays information about dynamic and static ND entries. The information helps you:

- Check whether the local routing device has learned MAC addresses from neighbors.
- Check the neighbor status of the local routing device, including neighbor unreachable, neighbor reachable, or unknown.

You can run one of the following commands as required:

- To view neighbor entries based on the neighbor IPv6 address, run the **display ipv6 neighbors** [*ipv6-address*] command.
- To view neighbor entries based on the neighbor interface number, run the **display ipv6 neighbors** *interface-type interface-number* command.

  To view neighbor entries on a VLANIF interface, run the **display ipv6 neighbors** [[**vid** *vlan-id*] *interface-type interface-number*] command or the **display ipv6 neighbors** [*interface-type interface-number* [**vid** *vid*]] command.
- To view neighbor entries on a QinQ or Dot1q termination sub-interface, run the **display ipv6 neighbors** [*interface-type interface-number* [**vid** *vid* [**cevid** *cevid*]]] command.

If no parameter is specified, the **display ipv6 neighbors** command displays all neighbor entries.

Example

Display neighbor entries on GE1/0/0.

```
<Huawei> display ipv6 neighbors gigabitethernet 1/0/0
------------------------------------------------------------------------------
IPv6 Address : FC00::1
Link-layer   : 0000-1201-0102          State : REACH
Interface    : GE5/0/3                 Age   : 0
VLAN         : -                     CEVLAN: -
```

 Copyright © Huawei Technologies Co., Ltd.

```
VPN name     :                      Is Router: FALSE
Secure FLAG  : UN-SECURE

IPv6 Address : FE80::82FB:6FF:FE35:45B6
Link-layer   : 80fb-0635-45b6                State : STALE
Interface    : GE0/0/2                       Age   : 53
VLAN         : -                          CEVLAN: -
VPN name     :                              Is Router: TRUE
Secure FLAG  : UN-SECURE
--------------------------------------------------------------------------------
Total: 2        Dynamic: 2        Static: 0
```

Display neighbor entries of IPv6 address FC00::2.

```
<Huawei> display ipv6 neighbors fc00::2
--------------------------------------------------------------------------------
IPv6 Address : FC00::2
Link-layer   : 00e0-fc89-fe6e          State : STALE
Interface    : GE1/0/0                 Age   : 7
VLAN         : -                     CEVLAN: -
VPN name     :                         Is Router: FALSE
Secure FLAG  : UN-SECURE
--------------------------------------------------------------------------------
Total: 1        Dynamic: 1         Static: 0
```

Display neighbor entries of IPv6 VPN instance **vpnA**.

```
<Huawei> display ipv6 neighbors vpn-instance vpnA
--------------------------------------------------------------------------------
IPv6 Address : FE80::2E0:FCFF:FE8C:417D
Link-layer   : 00e0-fc8c-417d          State : STALE
Interface    : Eth4/2/0                Age   : #
VLAN         : -                     CEVLAN: -
VPN name     : vpnA                    Is Router: FALSE
Secure FLAG  : UN-SECURE

IPv6 Address : FE80::2E0:FCFF:FE95:DD66
Link-layer   : 00e0-fc95-dd66          State : STALE
Interface    : Eth4/2/0                Age   : #
VLAN         : -                     CEVLAN: -
VPN name     : vpnA                    Is Router: FALSE
--------------------------------------------------------------------------------
Total: 2        Dynamic: 2        Static: 0
```

Table 8-84 Description of the display ipv6 neighbors command output

Item	Description
IPv6 Address	IPv6 address of a neighbor.
Link-layer	Link layer address (MAC address) of a neighbor.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
State	Status of a neighbor entry: ● INCMP: indicates that the neighbor is unreachable. When the address is being resolved, the link layer address of the neighbor is not detected. If resolution succeeds, the neighbor entry is in REACH state. ● REACH: indicates that the neighbor is reachable within a specified period. By default, the neighbor is reachable within 30s. If the period expires and the entry remains unused, the neighbor entry is in STALE state. ● STALE: indicates that whether the neighbor is reachable is unknown. The entry remains unused within a specified period. By default, the neighbor is reachable within 30s. A device does not detect neighbor reachability unless it needs to send packets to a neighbor. ● DELAY: indicates that whether the neighbor is reachable is unknown. A device has sent a packet to a neighbor. If the device does not receive any response from the neighbor within the specified period, the neighbor entry is in PROBE state. ● PROBE: indicates that whether the neighbor is reachable is unknown. A device has sent a packet to a neighbor to detect whether the neighbor is reachable. If the device receives a response from the neighbor within a specified period, the neighbor entry is in REACH state. Otherwise, the neighbor entry is in INCMP state.
Interface	Name of the interface to which the neighbor entry belongs.
Age	Aging time of the neighbor entry: ● The aging time of static entries is displayed as "-". ● The aging time of dynamic entries is the time elapsed since the neighbor becomes reachable, in minutes. If the neighbor is always unreachable, "#" is displayed (only for dynamic entries).
VLAN	ID of the VLAN to which the neighbor belongs.
VPN name	Name of a VPN instance to which the neighbor belongs.
CEVLAN	Inner VLAN ID.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Is Router	Whether an NA packet carries the R flag: • If the NA packet carries the R flag, "TRUE" is displayed. In this case, the neighbor is a routing device. • If the NA packet carries no R flag, "FALSE" is displayed. In this case, the neighbor may be a PC or a routing device that sends an NA packet carrying no R flag.
Secure FLAG	Whether the neighbor entry is secure: • If the neighbor entry is static or the neighbor has the neighbor security function enabled, "SECURE" is displayed. • If the neighbor entry is dynamic and the neighbor has no neighbor security function enabled, "UN-SECURE" is displayed.
Total	Total number of neighbor entries.
Dynamic	Number of dynamic neighbor entries.
Static	Number of static neighbor entries.

Related Topics

8.8.54 ipv6 neighbor

8.8.11 display ipv6 pathmtu

Function

The **display ipv6 pathmtu** command displays information about PMTU entries.

Format

display ipv6 pathmtu [**vpn-instance** *vpn-instance-name*] { *ipv6-address* | **all** | **dynamic** | **static** }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays PMTU entries of a specified IPv6 VPN instance.	The value must be an existing VPN instance.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ipv6-address	Displays PMTU entries of a specified IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
all	Displays all PMTU entries.	-
dynamic	Displays all dynamic PMTU entries.	-
static	Displays all static PMTU entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The path MTU (PMTU) discovery mechanism determines the maximum size of packets that can be transmitted on a path.

The **display ipv6 pathmtu** command displays information about dynamic and static PMTU entries. The device then fragments packets into a size smaller than the PMTU and forwards the fragmented packets.

Precautions

If no PMTU is set using the **8.8.55 ipv6 pathmtu** command, no static PMTU entry is displayed after the **display ipv6 pathmtu** command is run.

Example

Display all PMTU entries.

```
<Huawei> display ipv6 pathmtu all
IPv6 Destination Address                ZoneID  PathMTU  LifeTime(M)  Type
FC00::1                                 0       1500     -            Static
------------------------------------------------------------------------------
Total: 1        Dynamic: 0      Static: 1
```

Display PMTU entries of VPN instance **vpn1**.

```
<Huawei> display ipv6 pathmtu vpn-instance vpn1 all
IPv6 Destination Address                ZoneID  PathMTU  LifeTime(M)  Type
FC00::1                                 1       1600     -            Static
------------------------------------------------------------------------------
Total: 1        Dynamic: 0      Static: 1
```


Copyright © Huawei Technologies Co., Ltd.

Table 8-85 Description of the display ipv6 pathmtu command output

Item	Description
Total	Total number of PMTU entries.
Dynamic	Total number of dynamic PMTU entries.
Static	Total number of static PMTU entries.
IPv6 Destination Address	Destination IPv6 address.
ZoneID	Zone ID.
PathMTU	PMTU of an IPv6 address.
LifeTime(M)	Remaining lifetime of dynamic PMTU entries, in minutes. This field displays "-" for static entries.
Type	Type of the PMTU entry: • Dynamic: dynamic entries • Static: static entries

Related Topics

8.8.56 ipv6 pathmtu age
8.8.55 ipv6 pathmtu

8.8.12 display ipv6 socket

Function

The **display ipv6 socket** command displays information about IPv6 sockets.

If no parameter is specified, this command displays information about all types of sockets.

Format

display ipv6 [**ha**] **socket** [**socktype** *socket-type* | **task-id** *task-id* **socket-id** *socket-id*]

Parameters

Parameter	Description	Value
ha	Displays IPv6 socket information on the slave main control board.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
socktype *socket-type*	Specifies the type of a socket. The value can be: • 1: indicates SOCK_STREAM, corresponding to the TCP-based socket. • 2: indicates SOCK_DGRAM, corresponding to the UDP-based socket. • 3: indicates SOCK_RAW, corresponding to the RawIP-based socket.	The value is an integer that ranges from 1 to 3.
socket-id *socket-id*	Specifies the socket ID.	The value is an integer that ranges from 1 to 131072.
task-id *task-id*	Specifies the task ID.	The value is an integer that ranges from 1 to 350.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To locate a fault, you can use this command to view detailed information about sockets of all types or a specified type.

Precautions

If there is no socket information, no information is displayed.

Example

Display information about a socket with a specified socket type, socket ID, and task ID.

```
<Huawei> display ipv6 socket
SOCK_STREAM:
Task = VTYD (14), socketid = 4, Proto = 6,
LA = ::->22, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT SO_SENDVPNID,
socket state = SS_PRIV SS_ASYNC
SOCK_DGRAM:
Task = VTYD (14), socketid = 3, Proto = 6,
LA = ::->23, FA = ::->0,
```

 Copyright © Huawei Technologies Co., Ltd.

```
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT SO_SENDVPNID,
socket state = SS_PRIV SS_ASYNC
```

Display information about the socket with socket type 1.

```
<Huawei> display ipv6 socket socktype 1
SOCK_STREAM:
Task = VTYD(14), socketid = 4, Proto = 6,
LA = ::->22, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT SO_SENDVPNID,
socket state = SS_PRIV SS_ASYNC
Task = VTYD(14), socketid = 3, Proto = 6,
LA = ::->23, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT SO_SENDVPNID,
socket state = SS_PRIV SS_ASYNC
```

Table 8-86 Description of the display ipv6 socket command output

Item	Description
SOCK_STREAM	One type of socket. Sockets are classified into the following types: • SOCK_STREAM • SOCK_DGRAM • SOCK_RAW
Task = VTYD(14)	Type and ID of the task that invokes the socket. For example, **Task = VTYD(14)** shows that the task named VTYD uses the socket, with task ID 14.
socketid = 4	Socket ID.
Proto = 6	Protocol ID.
LA = ::->22, FA = ::->0	• LA: indicates the local address and local port number. • FA: indicates the remote address and remote port number.
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,	• sndbuf: indicates the upper limit of the send buffer, in bytes. • rcvbuf: indicates the upper limit of the receive buffer, in bytes. • sb_cc: indicates the total number of sent bytes. • rb_cc: indicates the total number of received bytes.
socket option	Socket option that has been set.
socket state	Socket status.

Copyright © Huawei Technologies Co., Ltd.

8.8.13 display ipv6 statistics

Function

The **display ipv6 statistics** command displays IPv6 traffic statistics.

Format

display ipv6 statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays IPv6 traffic statistics on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display ipv6 statistics** command to view statistics on received and sent IPv6 packets.

During packet transmission, if the source node has fragmented packets, you can run this command to view the total number of IPv6 packets that are successfully fragmented and the total number of fragmented packets that have been sent, and then check whether the number of fragmented packets received by the destination node is correct.

Precautions

The total number of packets received by the device includes the number of forwarded packets, number of packets delivered by the routing device to the upper layer, and number of discarded packets.

Example

Display IPv6 traffic statistics on the device.

```
<Huawei> display ipv6 statistics
IPv6 Protocol:
  Sent packets:
```

 Copyright © Huawei Technologies Co., Ltd.

```
  Total              : 2
  Local sent out     : 2          Forwarded          : 0
  Raw packets        : 0          Discarded          : 0
  Fragmented         : 0          Fragments          : 0
  Fragments failed   : 0          Multicast          : 2
Received packets:
  Total              : 0          Local host         : 0
  Hop count exceeded : 0          Header error       : 0
  Too big            : 0          Routing failed     : 0
  Address error      : 0          Protocol error     : 0
  Truncated          : 0          Option error       : 0
  Fragments          : 0          Reassembled        : 0
  Reassembly timeout : 0          Multicast          : 0
  Fragments overlap  : 0
  Extension header:
    Hop-by-hop options  : 0             Mobility header      : 0

    Destination options : 0             Routing header       : 0

    Fragment header     : 0             Authentication header : 0

    Encapsulation header : 0            No header            : 0

    TLV length error    : 0             Header length error  : 0

    Unknown header type : 0             Unknown TLV type     : 0
```

Table 8-87 Description of the display ipv6 statistics command output

Item	Description
Sent packets	Statistics about sent packets.
Total	Total number of sent packets.
Local sent out	Total number of packets sent by the local device.
Forwarded	Number of forwarded packets.
Raw packets	Total number of packets sent through the raw socket, such as ping or tracert packets.
Discarded	Total number of discarded packets.
Fragmented	Total number of IPv6 packets that are successfully fragmented.
Fragments	Total number of sent fragmented packets.
Fragments failed	Total number of IPv6 packets that fail to be fragmented.
Multicast	Total number of sent multicast packets.
Received packets	Statistics about received packets.
Total	Total number of received packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Local host	Total number of packets received by the local device.
Hop count exceeded	Total number of packets whose hops exceed the upper limit.
Header error	Total number of packets with incorrect packet header.
Too big	Total number of received packets that fail to be forwarded because of excessive size.
Routing failed	Total number of packets that fail to be routed.
Address error	Total number of packets with incorrect IP addresses.
Protocol error	Total number of packets with the incorrect protocol.
Truncated	Total number of packets discarded because the actual packet length is shorter than that specified in the packet length field.
Option error	Total number of packets that carry incorrect options.
Fragments	Total number of received fragmented packets.
Reassembled	Total number of packets that are successfully reassembled.
Reassembled timeout	Total number of packets that fail to be reassembled due to timeout.
Multicast	Total number of received multicast packets.
Fragments overlap	Total number of received fragmented packets that are overlapped.
Extension Header	Total count of the IPv6 extension headers
Hop-by-Hop Options	Total count of the hop-by-hop options headers
Mobility Header	Total count of the mobility headers
Destination Options	Total count of the destination options headers

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Routing Header	Total count of the routing options headers
Fragment Header	Total count of the fragment headers
Authentication Header	Total count of the authentication headers
Encapsulation Header	Total count of the encapsulation headers
No header	Total count of the packets without headers
TLV Length error	Total count of the extension headers in which the TLV length field is wrong
Header Length error	Total count of the extension headers in which the length field is wrong.
Unknown header type	Total count of the unknown extension header types
Unknown TLV type	Total count of the unknown TLV types

Related Topics

8.8.63 reset ipv6 statistics

8.8.14 display rawip ipv6 statistics

Function

The **display rawip ipv6 statistics** command displays Raw IPv6 packet statistics.

Format

display rawip ipv6 statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run the **display rawip ipv6 statistics** command to view Raw IPv6 packet statistics, including:

- Statistics about received and sent Raw IPv6 packets
- Statistics about discarded Raw IPv6 packets

Example

Display Raw IPv6 packet statistics.

```
<Huawei> display rawip ipv6 statistics
 Received packets:
    total: 20
    packets sent for external pre processing: 0
    packets for which checksum has to be calculated: 0
    packets with invalid checksum : 0
    dropped packets due to socket buffer is full: 0
    dropped packets due to no matching socket: 20
    dropped multicast packets due to no matching socket: 0
 Sent packets:
    total (excluding ICMP6 packets): 0
```

Table 8-88 Description of the display rawip ipv6 statistics command output

Item	Description
total	Total number of received and sent packets.
packets sent for external pre processing	Number of received Raw IPv6 packets for external preprocessing.
packets for which checksum has to be calculated	Number of received Raw IPv6 packets for which checksum has been calculated.
packets with invalid checksum	Number of discarded Raw IPv6 packets with checksum errors.
dropped packets due to socket buffer is full	Number of Raw IPv6 packets that are discarded because the socket buffer is full.
dropped packets due to no matching socket	Number of discarded Raw IPv6 packets that do not match the receiving socket.
dropped multicast packets due to no matching socket	Number of discarded Raw IPv6 packets destined to a multicast address that do not match the receiving socket.

8.8.15 display tcp ipv6 authentication-statistics

Function

The **display tcp ipv6 authentication-statistics** command displays authentication statistics of a specified TCP6 connection.

 Copyright © Huawei Technologies Co., Ltd.

Format

display tcp ipv6 authentication-statistics src-ip *src-ip* **src-port** *src-port* **dest-ip** *dest-ip* **dest-port** *dest-port*

Parameters

Parameter	Description	Value
src-ip *src-ip*	Specifies the source IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
src-port *src-port*	Specifies the source port.	The value is an integer that ranges from 0 to 65535.
dest-ip *dest-ip*	Specifies the destination IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
dest-port *dest-port*	Specifies the destination port.	The value is an integer that ranges from 0 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display tcp ipv6 authentication-statistics** command to view authentication statistics of a specified TCP6 connection, including:

- Number of TCP6 packets with MD5 Option
- Number of TCP6 packets with Enhanced Authentication Option

Example

Display authentication statistics of a specified TCP6 connection.

```
<Huawei> display tcp ipv6 authentication-statistics src-ip fc00::1 src-port 3456 dest-ip fc00::5 dest-port 5678
MD5 Signature Option (MSO)is enabled |
 Enhanced Authentication Option (EAO)is enabled
Received packets:
    total: 0
    packets received with MSO: 0
    packets received with EAO: 0
    packets dropped due to MD5 authentication failure: 0
    packets dropped due to absence of MSO: 0
    packets dropped due to presence of MSO: 0
    packets dropped due to MAC authentication failure: 0
```

 Copyright © Huawei Technologies Co., Ltd.

```
    packets dropped due to absence of active receive key: 0
    packets dropped due to invalid receive algorithm id: 0
    packets dropped due to absence of EAO: 0

Sent packets:
    total: 0
    packets sent with MSO: 0
    packets sent with EAO: 0
    packets not sent due to absence of active send key: 0
```

Table 8-89 Description of the display tcp ipv6 authentication-statistics command output

Item	Description
packets received with MSO	Total number of received TCP6 packets with MD5 Option.
packets received with EAO	Total number of received TCP6 packets with Enhanced Authentication Option.
packets dropped due to MD5 authentication failure	Total number of TCP6 packets discarded due to MD5 authentication failure.
packets dropped due to absence of MSO	Total number of TCP6 packets discarded due to absence of MD5 Option.
packets dropped due to presence of MSO	Total number of TCP6 packets discarded due to presence of MD5 Option.
packets dropped due to MAC authentication failure	Total number of TCP6 packets discarded due to MAC authentication failure.
packets dropped due to absence of active receive key	Total number of TCP6 packets discarded due to absence of active receive key.
packets dropped due to invalid receive algorithm id	Total number of TCP6 packets discarded due to invalid receive algorithm ID.
packets dropped due to absence of EAO	Total number of TCP6 packets discarded due to absence of Enhanced Authentication Option.
packets sent with MSO	Total number of sent TCP6 packets with MD5 Option.
packets sent with EAO	Total number of sent TCP6 packets with Enhanced Authentication Option.
packets not sent due to absence of active send key	Total number of TCP6 packets discarded due to absence of active send key.

Related Topics

8.8.65 reset tcp ipv6 authentication-statistics

Copyright © Huawei Technologies Co., Ltd.

8.8.16 display tcp ipv6 statistics

Function

The **display tcp ipv6 statistics** command displays IPv6 TCP traffic statistics.

Format

display tcp ipv6 statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can check the network connection status according to the items in the command output:

- Established connections: You can view information about "Established connections" to check whether the number of connections exceeds the upper limit, and then determine whether to continue deploying services or adjust the load.
- Duplicate ACK packets: You can view information about "Duplicate ACK packets" to check whether the device is attacked by unknown ACK packets. If the device receives a large number of unknown ACK packets, the device may be attacked.
- Out-of-order packets: You can view information about "Out-of-order packets" to check network performance. If the network is in poor condition, a lot of out-of-order packets are generated.

Precautions

- The total number of received packets includes the number of forwarded packets, number of packets delivered to the upper layer, and number of discarded packets.
- Before running this command to view IPv6 TCP statistics within a specified period, run the **8.8.66 reset tcp ipv6 statistics** command to clear existing statistics.

Example

Display IPv6 TCP packet statistics.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display tcp ipv6 statistics
Received packets:
    total: 0
    total(64bit high-capacity counter): 0
    packets in sequence: 0 (0 bytes)
    window probe packets: 0
    window update packets: 0
    checksum error: 0
    offset error: 0
    short error: 0
    duplicate packets: 0 (0 bytes)
    partially duplicate packets: 0 (0 bytes)
    out-of-order packets: 0 (0 bytes)
    packets with data after window: 0 (0 bytes)
    packets after close: 0
    ACK packets: 0 (0 bytes)
    duplicate ACK packets: 0
    too much ACK packets: 0
    packets dropped due to MD5 authentication failure: 0
    packets dropped due to absence of MSO: 0
    packets dropped due to presence of MSO: 0
    packets received with MD5 Signature Option: 0
    packets dropped due to MAC authentication failure: 0
    packets dropped due to absence of active receive key: 0
    packets dropped due to invalid receive algorithm id: 0
    packets dropped due to absence of Enhanced Authentication Option: 0
    packets received with Enhanced Authentication Option: 0

Sent packets:
    total: 0
    urgent packets: 0
    total(64bit high-capacity counter): 0
    control packets: 0 (including 0 RST)
    window probe packets: 0
    window update packets: 0
    data packets: 0 (0 bytes)
    data packets retransmitted: 0 (0 bytes)
    ACK only packets: 0 (0 delayed)
    packets sent with MD5 Signature Option: 0
    packets sent with Enhanced Authentication Option: 0
    packets not sent due to absence of active send key: 0

Other Statistics:
    retransmitted timeout: 0
    connections dropped in retransmitted timeout: 0
    keepalive timeout: 0
    keepalive probe: 0
    keepalive timeout, so connections disconnected: 0
    initiated connections: 0
    accepted connections: 0
    established connections: 0
    closed connections: 0 (dropped: 0, initiated dropped: 0)
```

Table 8-90 Description of the display tcp ipv6 statistics command output

Item	Description
Received packets: total: 0	Total number of received packets.
total(64bit high-capacity counter)	Total number of received or sent packets counted by the 64-bit high-capacity counter.
packets in sequence	Number of packets received in sequence.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
window probe packets	Number of received window probe packets.
window update packets	Number of received window update packets.
checksum error	Number of received packets with invalid checksum.
offset error	Number of received packets with incorrect TCP header length.
short error	Number of received packets with total length shorter than the set value in the packet header.
duplicate packets	Number of received duplicate packets.
partially duplicate packets	Number of received partially duplicate packets.
out-of-order packets	Number of received out-of-order packets.
packets with data after window	Number of received packets exceeding the receive window.
packets after close	Number of packets received after the connection is closed.
ACK packets	Number of received ACK packets.
duplicate ACK packets	Number of received duplicate ACK packets.
too much ACK packets	Number of received ACK packets with too large ACK values.
packets dropped due to MD5 authentication failure	Number of packets discarded due to MD5 authentication failure.
packets dropped due to absence of MSO	Number of packets discarded due to absence of MD5 Signature Option.
packets dropped due to presence of MSO	Number of packets discarded due to presence of MD5 Signature Option.
packets received with MD5 Signature Option	Number of received packets with MD5 Signature Option.
packets dropped due to MAC authentication failure	Number of packets discarded due to MAC authentication failure.
packets dropped due to absence of active receive key	Number of packets discarded due to absence of active receive key.
packets dropped due to invalid receive algorithm id	Number of packets discarded due to invalid receive algorithm ID.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
packets dropped due to absence of Enhanced Authentication Option	Number of packets discarded due to absence of Enhanced Authentication Option.
packets received with Enhanced Authentication Option	Number of received packets with Enhanced Authentication Option.
Sent packets: total: 0	Total number of sent packets.
urgent packets	Number of sent packets with the urgent pointer.
control packets	Number of sent control packets.
window probe packets	Number of sent window probe packets.
window update packets	Number of sent window update packets.
data packets	Number of sent data packets.
data packets retransmitted	Number of retransmitted data packets.
ACK only packets	Number of sent ACK only packets.
packets sent with MD5 Signature Option	Number of sent packets with MD5 Signature Option.
Other Statistics:	Other statistics.
retransmitted timeout	Number of retransmission timeout packets.
connections dropped in retransmitted timeout	Number of disconnected connections during the retransmission timeout.
keepalive timeout	Number of Keepalive timeouts.
keepalive probe	Number of Keepalive probes.
keepalive timeout, so connections disconnected	Number of connections disconnected due to Keepalive timeout.
initiated connections	Number of initiated connections.
accepted connections	Number of accepted connections.
established connections	Number of established connections.
closed connections	Number of closed connections.
dropped	Number of disconnected connections.
initiated dropped	Number of initiated and disconnected connections.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

8.8.66 reset tcp ipv6 statistics

8.8.17 display tcp ipv6 status

Function

The **display tcp ipv6 status** command displays the status of all IPv6 TCP connections.

Format

display tcp ipv6 status [**local-ip** *ipv6-address*] [**local-port** *local-port*] [**remote-ip** *ipv6-address*] [**remote-port** *remote-port*]

display tcp ipv6 status [**task-id** *task-id* [**sock-id** *sock-id*]]

Parameters

Parameter	Description	Value
local-ip *ipv6-address*	Displays the IPv6 TCP connection status of the specified IPv6 address. *ipv6-address* specifies the IPv6 address of the local device.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
local-port *local-port*	Displays the IPv6 TCP connection status of the specified port number. *local-port* specifies the port number of the local device.	The value is an integer that ranges from 0 to 65535.
remote-ip *ipv6-address*	Displays the IPv6 TCP connection status of the specified IPv6 address. *ipv6-address* specifies the IPv6 address of the remote device.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
remote-port *remote-port*	Displays the IPv6 TCP connection status of the specified port number. *remote-port* specifies the port number of the remote device.	The value is an integer that ranges from 0 to 65535.
task-id *task-id*	Displays the status of the IPv6 TCP connection with the specified task ID. *task-id* specifies the task ID.	The value is an integer that ranges from 1 to 200.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
sock-id *sock-id*	Displays the status of the IPv6 TCP connection with the specified socket ID.	The value is an integer that ranges from 1 to 131072.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display tcp ipv6 status** command to view all valid IPv6 TCP control blocks, including the following information:

- IPv6 TCP socket ID
- APP CID
- Local IPv6 address and port number
- Remote IPv6 address and port number
- IPv6 TCP connection status
- VPN ID

To view the status of all valid IPv6 TCP connections, run the **display tcp ipv6 status** [**local-ip** *ipv6-address*] [**local-port** *local-port-number*] [**remote-ip** *ipv6-address*] [**remote-port** *remote-port-number*] command.

To view the status of the IPv6 TCP connection with a specified socket ID, run the **display tcp ipv6 status** [**task-id** *task-id* [**sock-id** *sock-id*]] command.

Precautions

If there is no TCP connection, no information is displayed.

Example

Display the status of IPv6 TCP connections.

```
<Huawei> display tcp ipv6 status
* - MD5 Authentication is enabled.
# - Keychain Authentication is enabled.
TCP6CB   TID/SoID  Local Address       Foreign Address     State       VPNID
19490ba4 9/2       ::->23              ::->0               Listening   23553
```

 Copyright © Huawei Technologies Co., Ltd.

Table 8-91 Description of the **display tcp ipv6 status** command output

Item	Description
TCP6CB	Address of an IPv6 TCP control block, in hexadecimal notation.
TID/SoID	Task ID and socket ID.
Local Address	Local IPv6 address and port number.
Foreign Address	Remote IPv6 address and port number.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
State	Status of an IPv6 TCP connection: • Closed: indicates that the TCP connection is closed. • Listening: indicates that the TCP connection is being listened on. • Syn_Rcvd: indicates that a TCP packet with the SYN flag is received. • Syn_Sent: indicates that a TCP packet with the SYN flag is sent. • Established: indicates that the TCP connection has been set up. • Close_Wait: indicates that a user host sends a packet with the FIN flag to the server, requesting the server to close the TCP connection in Established state. The server then sends an ACK packet to the user host after receiving the packet and enters the Close_Wait state. • Fin_Wait1: indicates that a user host sends a packet with the FIN flag to the server, requesting the server to close the TCP connection and enters the Fin_Wait1 state. • Fin_Wait2: indicates that a user host receives an ACK packet in a response to the sent packet with the FIN flag and enters the Fin_Wait2 state. • Time_Wait: indicates that TCP enters this state after the TCP connection is closed. When TCP has been in Time_Wait state two times the longest packet lifetime, records about the closed connection are deleted. • Closing: indicates that the two ends close the TCP connection simultaneously. • LAST_ACK: indicates that the local end waits for acknowledging the TCP connection teardown request sent to the remote end.
VPNID	VPN interface ID.

 Copyright © Huawei Technologies Co., Ltd.

8.8.18 display this ipv6 interface

Function

The **display this ipv6 interface** command displays IPv6 information on the current interface.

Format

display this ipv6 interface

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

After an IPv6 address is configured in the interface view, you can run the **display this ipv6 interface** command to check IPv6 information on the interface.

Example

Display IPv6 information on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] display this ipv6 interface
GigabitEthernet1/0/0 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::2E0:4AFF:FE3D:9801
  Global unicast address(es):
    2001::1, subnet is 2001::/64
  Joined group address(es):
    FF02::1:FF00:1
    FF02::1:FF3D:9801
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND stale time is 1200 seconds
  Hosts use stateless autoconfig for addresses
```

Table 8-92 Description of the display this ipv6 interface command output

Item	Description
GigabitEthernet1/0/0 current state	Current physical status of GE1/0/0.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
IPv6 protocol current state	Current protocol status of the interface.
link-local address	Link-local address configured on the interface.
Global unicast address(es)	Global unicast address configured on the interface.
Joined group address(es)	Addresses of all multicast groups that the interface joins.
MTU	MTU of the interface.
number of DAD attempts	Number of times duplicate address detection is performed.
ND reachable time	Neighbor reachable time.
ND retransmit interval	Retransmission interval.
Hosts use stateless autoconfig for addresses	Hosts obtain addresses using stateless autoconfiguration.
ND stale time	Time period for the neighbor to keep the STALE state.

Related Topics

8.8.8 display ipv6 interface

8.8.19 display udp ipv6 statistics

Function

The **display udp ipv6 statistics** command displays IPv6 UDP packet statistics.

Format

display udp ipv6 statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The User Datagram Protocol (UDP) is a simple protocol that exchanges packets on the Internet. You can run the **display udp ipv6 statistics** command to view statistics about sent and received IPv6 UDP packets.

Precautions

The total number of packets received by the device includes the number of forwarded packets, number of packets delivered by the device to the upper layer, and number of discarded packets.

Example

Display IPv6 UDP packet statistics.

```
<Huawei> display udp ipv6 statistics
Received packets:
    total: 0
    total(64bit high-capacity counter): 0
    checksum error: 0
    shorter than header: 0
    invalid message length: 0
    no socket on port: 0
    no multicast port: 0
    not delivered, input socket full: 0
    input packets missing pcb cache: 0
    packets sent for external pre processing: 0

Sent packets:
    total: 0
    total(64bit high-capacity counter): 0
```

Table 8-93 Description of the display udp ipv6 statistics command output

Item	Description
Received packets	Number of received packets.
total	Total number of received and sent packets.
checksum error	Total number of packets with invalid checksum.
shorter than header	Total number of IPv6 UDP packets with the length shorter than the packet header.
invalid message length	Total number of packets whose data length is longer than the packet length.
no socket on port	Number of packets without corresponding sockets on the interface.
no multicast port	Number of received packets carrying nonexistent multicast interfaces.
not delivered, input socket full	Number of unprocessed packets when the buffer is full.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
input packet missing pcb cache	Number of received packets failing to find the PCB cache.
packets sent for external pre processing	Number of received packets for external preprocessing.
Sent packets	Number of sent packets.

8.8.20 ipv6

Function

The **ipv6** command enables the device to forward IPv6 unicast packets, including sending and receiving local IPv6 packets.

The **undo ipv6** command disables the device from forwarding IPv6 unicast packets.

By default, a device is disabled from forwarding IPv6 unicast packets.

Format

ipv6

undo ipv6

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You must run the **ipv6** command in the system view before performing IPv6 configurations.

Example

Enable the device to forward IPv6 unicast packets.

```
<Huawei> system-view
[Huawei] ipv6
```

Disable the device from forwarding IPv6 unicast packets.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] undo ipv6
Warning: This operation will interrupt all IPv6 services. Continue?[Y/N]:y
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.21 ipv6 address

Function

The **ipv6 address** command configures a global unicast address for an interface.

The **ipv6 address** *dhcpv6-prefix* command configures an IPv6 address bound to the DHCPv6 PD prefix for an interface.

The **undo ipv6 address** command deletes a global unicast address from an interface.

The **undo ipv6 address** *dhcpv6-prefix* command deletes the IPv6 address bound to the DHCPv6 PD prefix for an interface.

By default, no global unicast address is configured for an interface.

By default, no IPv6 address bound to the DHCPv6 PD prefix is configured for an interface.

Format

ipv6 address { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* }

ipv6 address *dhcpv6-prefix* { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* }

undo ipv6 address [*ipv6-address prefix-length* | *ipv6-address*/*prefix-length*]

undo ipv6 address *dhcpv6-prefix*

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of an interface.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
prefix-length	Specifies the prefix length of an IPv6 address.	The value is an integer that ranges from 1 to 128.
dhcpv6-prefix	Specifies the prefix assigned to a DHCPv6 PD client.	The value is a string of 1to 63 characters.

Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A global unicast address is similar to an IPv4 public network address. Global unicast addresses are used on the links that can be summarized, and are provided for the Internet Service Providers (ISPs). These addresses allow route prefix summarization, limiting global routing entries. A global unicast address consists of a 48-bit route prefix managed by carriers, a 16-bit subnet ID managed by local nodes, and a 64-bit interface ID.

The device is required to function as a DHCPv6 PD client and obtain an IPv6 address prefix from the DHCPv6 PD server. You can run the **ipv6 address** *dhcpv6-prefix* { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* } command to configure an IPv6 address is bound to the DHCPv6 PD prefix. After you run this command, the device uses the prefix assigned to the DHCPv6 PD client and the IPv6 address to form an RA prefix for the interface only when the device functions as a DHCPv6 PD client and obtains a prefix. The prefix must be a 64-digit number. If not, the host cannot use this prefix for automatic assignment of IPv6 addresses.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

The following conditions are prohibited for different interfaces on the same device:

- The IPv6 addresses are the same.
- The network prefixes of the IPv6 addresses are the same. For example, if the IPv6 address of interface A is 2001:db8::1/12 and its network prefix is 200:: and the IPv6 address of interface B is 2001:db8::1/127 and its network prefix is 2001:db8::, the configuration succeeds. If the IPv6 address of interface B is also 2002:db8::1/12 and its network prefix is also 200::, the configuration fails.
- A device functions as a DHCPv6 PD client and obtains an IPv6 address prefix from a DHCPv6 PD server. You can run the **ipv6 address** *dhcpv6-prefix*{ *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* }command to configure an IPv6 address bound to a DHCPv6 prefix on an interface. For example, if the ipv6 address dhcpv6-prefix1 ::1:0:0:0:1/64 and ipv6 address dhcpv6-prefix1 ::1:0:0:0:2/64 commands are configured on interfaces A and B respectively, the network prefixes of interfaces A and B are the same. As a result, the configuration is successful but takes effect only on one interface. If the preceding case occurs, check whether any address conflict exists.

A maximum of 10 global unicast addresses can be configured for an interface.

An IPv6 address with a 128-bit prefix can be configured only on a loopback interface.

 Copyright © Huawei Technologies Co., Ltd.

After the **ipv6 address** command is run to configure a global unicast address for an interface, the system generates a link-local address for the interface, if no link-local address is configured for the interface.

If no parameter (IPv6 address or prefix length) is specified in the **undo ipv6 address** command, all IPv6 addresses configured for the interface are deleted after the command is run.

Example

Configure global unicast address 2001::1/64 for GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 address 2001::1 64
```

Configure an IPv6 address bound to the DHCPv6 PD prefix for GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 address prefix1 ::1:0:0:0:1/64
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.22 ipv6 address anycast

Function

The **ipv6 address anycast** command configures an IPv6 anycast address.

The **undo ipv6 address** command deletes an IPv6 anycast address.

By default, no IPv6 anycast address is configured.

Format

ipv6 address { *ipv6-address prefix-length* | *ipv6-address*|*prefix-length* } **anycast**

undo ipv6 address [*ipv6-address prefix-length* | *ipv6-address*|*prefix-length*]

Parameters

Parameter	Description	Value
ipv6-address	Specifies an IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
prefix-length	Specifies the prefix length of an IPv6 address.	The value is an integer that ranges from 1 to 128.

Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An anycast address identifies a group of interfaces, which usually belong to different nodes. Packets sent to an anycast address are delivered to the nearest interface that is identified by the anycast address, depending on the routing protocols.

To implement communication between a 6to4 network and a local (native) IPv6 network using a 6to4 tunnel, configure an anycast address with prefix 2002:c058:6301:: for the tunnel interface of a 6to4 relay agent.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

If no parameter is specified in the **undo ipv6 address** command, all IPv6 addresses except link-local addresses are deleted.

An anycast address cannot be used as the source address of a packet. Therefore, a global unicast address must be configured when a device needs to send packets.

An IPv6 address with a 128-bit prefix can be configured only on a loopback interface.

Example

Configure anycast address fc00:c058:6301::/48 for Tunnel0/0/1.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol ipv6-ipv4 6to4
[Huawei-Tunnel0/0/1] ipv6 enable
[Huawei-Tunnel0/0/1] ipv6 address fc00:c058:6301:: 48 anycast
```

Related Topics

8.8.8 display ipv6 interface

8.8.28 ipv6 enable (interface view)

Copyright © Huawei Technologies Co., Ltd.

8.8.23 ipv6 address auto global

Function

The **ipv6 address auto global** command enables a device to generate an IPv6 global address through stateless autoconfiguration.

The **undo ipv6 address auto global** command disables a device from generating an IPv6 global address through stateless autoconfiguration.

By default, the device is disabled from generating an IPv6 global address through stateless autoconfiguration.

Format

ipv6 address auto global [**local-identifier**] [**default**]

undo ipv6 address auto global

Parameters

Parameter	Description	Value
default	Indicates that the device learns the default route.	-
local-identifier	Indicates the interface identifier of a local link address based on which a global address is generated.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **ipv6 address auto global** command is run, a device automatically generates an IPv6 global unicast address on the interface that receives a RA packet. The generated IPv6 address contains the address prefix in the received RA packet and interface identifier of the device. If the device does not receive RA packets, the device can only automatically configures a link-local address to interconnect with local nodes.

- If the **local-identifier** parameter is not specified, an interface identifier is generated in EUI-64 mode, and this identifier works together with the prefix in RA packets to composite a global address.
- If the **local-identifier** parameter is not specified, the interface identifier of the local link address is used to work together with the prefix in RA packets to composite a global address.

 Copyright © Huawei Technologies Co., Ltd.

A local link address can be generated either statically or dynamically. If the local link address is generated dynamically, this mode equals the EUI-64 mode, and the global address generated in this way is the same as that with the **local-identifier** parameter is specified. If the local link address is statically configured, the interface identifier of the global address is from the configuration of the local link address, which is different from the result with the **local-identifier** parameter not specified. You can choose the generation mode as required.

After the **ipv6 address auto global default** command is run, a device generates an IPv6 address based on the received RA packet and learns the source address in the RA packet. The device then uses the source IPv6 address as the next hop address of the default IPv6 route.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

After the **ipv6 address auto global** command is run, if an interface receives a new RA packet, a new IPv6 address is generated for the interface based on the received RA packet, but the default routes learned by the interface are not deleted.

If an interface has been configured with an IPv6 address, the original IPv6 address is not deleted after the interface receives an RA packet and generates a new IPv6 address. If the interface receives no RA packet and the generated IPv6 address expires, the interface deletes the generated IPv6 address and uses the original IPv6 address.

A device learns a maximum of three default routes based on RA packets. New routes cannot override the existing three routes, and extra routes will be discarded. If multiple default routes have the same priority, packets are forwarded in load balancing mode.

Example

Enable a device to generate an IPv6 global address through stateless autoconfiguration on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 address auto global local-identifier
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.24 ipv6 address auto link-local

Function

The **ipv6 address auto link-local** command configures an interface to automatically generate a link-local address.

Copyright © Huawei Technologies Co., Ltd.

The **undo ipv6 address auto link-local** command deletes the automatically generated link-local address.

By default, no link-local address is automatically generated on an interface.

Format

ipv6 address auto link-local

undo ipv6 address auto link-local

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an interface automatically obtains a link-local address, it can implement neighbor discovery and automatically configure a global unicast address or a unique local address.

Prerequisites

Before running this command, run the **ipv6 enable** command in the interface view to enable the IPv6 function.

Example

Configure GE1/0/0 to automatically generate a link-local address.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 address auto link-local
```

8.8.25 ipv6 address eui-64

Function

The **ipv6 address eui-64** command configures a global unicast address in EUI-64 format for an interface.

The **undo ipv6 address eui-64** command deletes a global unicast address in EUI-64 format from an interface.

 Copyright © Huawei Technologies Co., Ltd.

By default, no global unicast address in EUI-64 format is configured for an interface.

Format

ipv6 address { *ipv6-address prefix-length* | *ipv6-address*|*prefix-length* } **eui-64**

undo ipv6 address { *ipv6-address prefix-length* | *ipv6-address*|*prefix-length* } **eui-64**

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of an interface.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
prefix-length	Specifies the prefix length of an IPv6 address.	The value is an integer that ranges from 1 to 128. In EUI-64 format, the value must be smaller than 64.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In IPv6, any IPv6 unicast address needs an interface identifier. The interface identifier is globally unique, similar to a 48-bit MAC address.

The interface identifier of an IPv6 host address uses the IEEE EUI-64 format. A 64-bit interface identifier is generated based on an existing MAC address; therefore, such an interface identifier is globally unique. These 64-bit interface identifiers are globally valid for addressing and uniquely identify each network interface. An interface automatically configures an IPv6 address based on the network prefix obtained from an RA packet and the interface identifier in EUI-64 format.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

The following conditions are prohibited for different interfaces on the same device:

- The IPv6 addresses are the same.

 Copyright © Huawei Technologies Co., Ltd.

- The network prefixes of the IPv6 addresses are the same. For example, if the IPv6 address of interface A is 2001:db8::1/12 and its network prefix is 200:: and the IPv6 address of interface B is 2001:db8::1/127 and its network prefix is 2001:db8::, the configuration succeeds. If the IPv6 address of interface B is also 2002:db8::1/12 and its network prefix is also 200::, the configuration fails.

A maximum of 10 global unicast addresses can be configured for an interface.

The **ipv6 address eui-64** command applies to GE interfaces and sub-interfaces, XGE interfaces and XGE sub-interfaces, Eth-Trunk interfaces and sub-interfaces, POS interfaces, loopback interfaces, and tunnel interfaces.

After the **ipv6 address eui-64** command is run to configure an IPv6 address in EUI-64 format for an interface, the system generates a link-local address for the interface, if no link-local address is configured for the interface.

The following IPv6 addresses in EUI-64 format cannot be configured for an interface:

- Loopback address (::1/128)
- Unspecified address (::/128)
- Multicast address
- Anycast address

The **ipv6 address** command is used to specify a 128–bit IP address. Using the **ipv6 address eui-64** command, you can specify the high-order 64 bits of an IPv6 address. The low-order 64 bits of an IP address are automatically generated in the EUI-64 format. Even when the low-order 64 bits are manually specified, the automatically generated ones will override them.

Example

Configure IPv6 address 2001::1/64 in EUI-64 format for GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 address 2001::1 64 eui-64
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.26 ipv6 address link-local

Function

The **ipv6 address link-local** command configures a link-local address for an interface.

The **undo ipv6 address link-local** command deletes a link-local address on an interface.

By default, no link-local address is configured for an interface.

Copyright © Huawei Technologies Co., Ltd.

Format

ipv6 address *ipv6-address* **link-local**

undo ipv6 address *ipv6-address* **link-local**

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of an interface.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X. When a link-local address is being configured, the prefix of the specified IPv6 address must match FE80::/10.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Link-local addresses are used for the communication between nodes on the same local link in neighbor discovery or stateless autoconfiguration.

You can run the **ipv6 address link-local** command to manually configure a link-local address for an interface.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

Avoid changing link-local addresses.

You can configure multiple IPv6 addresses but only one link-local address for an interface.

The link-local address configured using the **ipv6 address link-local** command will override the link-local address automatically generated by the system.

The following IPv6 addresses cannot be configured for an interface:

- Loopback address (::1/128)
- Unspecified address (::/128)
- Multicast address
- Anycast address

 Copyright © Huawei Technologies Co., Ltd.

- IPv4-mapped IPv6 address (0:0:0:0:0:FFFF:IPv4-address)

Example

Configure link-local address fe80::1 for GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 address fe80::1 link-local
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.27 ipv6 address-policy

Function

The **ipv6 address-policy** command configures address selection policies.

The **undo ipv6 address-policy** command deletes address selection policies.

By default, the system has only default address selection policy entries. These entries are prefixed with ::1, ::, 2002::, FC00::, and ::FFFF:0.0.0.0.

Format

ipv6 address-policy [**vpn-instance** *vpn-instance-name*] *ipv6-address prefix-length precedence label*

undo ipv6 address-policy [**vpn-instance** *vpn-instance-name*] *ipv6-address prefix-length*

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance.
ipv6-address	Specifies an IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
prefix-length	Specifies the prefix length of an IPv6 address.	The value is an integer that ranges from 0 to 128.
precedence	Specifies the priority of an IPv6 address when the address is used as a destination address.	The value is an integer that ranges from 0 to 4294967295.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
label	Specifies the priority of an IPv6 address when the address is used as a source address.	The value is an integer that ranges from 0 to 4294967295.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When source and destination addresses need to be specified and planned, you can use this command to define a group of policies for selecting addresses. These address selection policies form a policy table. This table is similar to a routing table, allowing you to perform a longest match lookup on address selection policy. An address is selected based on the source and destination addresses.

- A source address is selected based on the *label* parameter. The address whose *label* value is the same as the *label* value of the destination address is preferred as the source address.
- A destination address is selected based on the *label* and *precedence* parameters. If *label* values of the candidate addresses are the same, the address with the largest *precedence* value is preferred as the destination address.

Precautions

The system supports a maximum of 50 address selection policy entries.

The default policy entries are those prefixed with ::1, ::, 2002::, FC00::, and ::FFFF:0.0.0.0.

Default policy entries cannot be created using a command.

Example

Set the priorities of IPv6 address FC00:1::/64 to 15 and 20 respectively when the address is used as a source address and a destination address.

```
<Huawei> system-view
[Huawei] ipv6 address-policy vpn-instance one fc00:1:: 64 15 20
```

Related Topics

8.8.6 display ipv6 address-policy

 Copyright © Huawei Technologies Co., Ltd.

8.8.28 ipv6 enable (interface view)

Function

The **ipv6 enable** command enables the IPv6 function on an interface.

The **undo ipv6 enable** command disables the IPv6 function on an interface.

By default, the IPv6 function is disabled on an interface.

Format

ipv6 enable

undo ipv6 enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can perform IPv6 configurations on an interface only when the interface has the IPv6 function enabled.

Prerequisites

The **ipv6** command has been run in the system view.

Precautions

The IPv6 function is not supported on MEth interfaces.

After the IPv6 function is disabled on an interface, IPv6 configurations on the interface are deleted. In addition, IS-IS IPv6 and RIPng are disabled on the interface. That is, the **isis ipv6 enable** and **ripng enable** commands become ineffective.

When the **ipv6 enable** command is run in the interface view, IPv6 is enabled on the interface. You can then perform IPv6 configurations on the interface. To configure an interface to forward IPv6 data, you must run the **ipv6** command in the system view to enable IPv6 forwarding. To enable an interface to forward IPv6 packets, you must enable IPv6 packet forwarding in the system view and interface view.

Copyright © Huawei Technologies Co., Ltd.

Example

Enable the IPv6 function on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
```

Related Topics

8.8.20 ipv6

8.8.29 ipv6 icmp blackhole unreachable send

Function

The **ipv6 icmp blackhole unreachable send** command enables the terminal access to send a Destination Unreachable ICMP packet to an initiator when a tracert packet matches an IPv6 blackhole route.

The **undo ipv6 icmp blackhole unreachable send** command disables the terminal access from sending a Destination Unreachable ICMP packet to an initiator when a tracert packet matches an IPv6 blackhole route.

By default, the terminal access is disabled from sending a Destination Unreachable ICMP packet to an initiator when a tracert packet matches an IPv6 blackhole route.

Format

ipv6 icmp blackhole unreachable send

undo ipv6 icmp blackhole unreachable send

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If static IPv6 blackhole routes are configured on the terminal access and a user goes offline, only the IPv6 blackhole route corresponding to the user's address segment exists on the terminal access. When a tracert packet matches the IPv6 blackhole route, the terminal access discards the packet. As a result, an initiator cannot detect that the user has gone offline.

 Copyright © Huawei Technologies Co., Ltd.

After you run the **ipv6 icmp blackhole unreachable send** command, the terminal access sends a Destination Unreachable ICMP packet to an initiator, notifying the initiator that the user has gone offline if a user goes offline and a tracert packet matches the IPv6 blackhole route.

Pre-configuration Tasks

Static IPv6 blackhole routes have been configured on the terminal access.

Example

Enable the terminal access to send a Destination Unreachable ICMP packet to an initiator when a tracert packet matches an IPv6 blackhole route.

```
<Huawei> system-view
[Huawei] ipv6 icmp blackhole unreachable send
```

Related Topics

8.7.18 icmp blackhole unreachable send

8.8.30 ipv6 icmp-error

Function

The **ipv6 icmp-error** command sets the rate limit for sending ICMPv6 error packets.

The **undo ipv6 icmp-error** command restores the default rate limit for sending ICMPv6 error packets.

By default, the size of the token buckets is 10 and the limit rate is 100 milliseconds.

Format

ipv6 icmp-error { **bucket** *bucket-size* | **ratelimit** *interval* } *

undo ipv6 icmp-error

Parameters

Parameter	Description	Value
bucket *bucket-size*	Specifies the maximum number of tokens the bucket can hold.	The value is an integer that ranges from 1 to 200. The default value is 10, which is recommended.
ratelimit *interval*	Specifies the interval for placing tokens into the bucket.	The value is an integer that ranges from 0 to 2147483647, in milliseconds. The default value is 100, which is recommended.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a network is not attacked, a routing device can correctly send ICMPv6 error packets to notify other devices of exceptions in packet transmission. If an attacker frequently sends ICMPv6 packets to network devices, the network devices will be busy responding with ICMPv6 packets. This affects system throughput and CPU usage. To prevent the system from sending a great number of ICMPv6 packets, run the **ipv6 icmp-error** command to limit the rate at which ICMPv6 packets are sent.

In the token bucket algorithm, one token represents an ICMPv6 packet. The system places tokens into the virtual bucket at a certain interval until the number of tokens in the bucket reaches the upper limit. When an ICMPv6 error packet is sent, a token is taken out of the token bucket. When there is no token, excess ICMPv6 error packets are discarded. You can limit the rate at which ICMPv6 packets are sent by setting the bucket size and the interval for placing tokens into the bucket.

Precautions

If you run the **ipv6 icmp-error** command multiple times, only the latest configuration takes effect.

If the interval for placing tokens into the bucket is 0, there is no limit on the interval.

Example

Set the rate limit for sending ICMPv6 error packets to 100.

```
<Huawei> system-view
[Huawei] ipv6 icmp-error ratelimit 100
```

Set the bucket size of ICMPv6 to 50.

```
<Huawei> system-view
[Huawei] ipv6 icmp-error bucket 50
```

Set the rate limit for sending ICMPv6 error packets to 100 and the bucket size to 50.

```
<Huawei> system-view
[Huawei] ipv6 icmp-error bucket 50 ratelimit 100
```

8.8.31 ipv6 icmp port-unreachable send

Function

The **ipv6 icmp port-unreachable send** command enables an interface to send ICMPv6 Port Unreachable messages.

The **undo ipv6 icmp port-unreachable send** command disables the function.

 Copyright © Huawei Technologies Co., Ltd.

By default, the enabling status of the function that the interface sends ICMPv6 Port Unreachable messages is the same as that of the function that the system sends ICMPv6 Port Unreachable messages.

Format

ipv6 icmp port-unreachable send

undo ipv6 icmp port-unreachable send

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a router receives a TCP6/UDP6 packet but cannot find the corresponding socket entry, the router replies with an ICMPv6 Port Unreachable message. This ICMPv6 error message carries the IPv6 address of the router as its source IPv6 address, which exposes the IPv6 address of the router and brings security risks. If the router is attacked by flooding packets, the router keeps replying with ICMPv6 Port Unreachable messages, causing high CPU usage and affecting device performance. To address this problem, run the **undo ipv6 icmp port-unreachable send** command on the inbound interface of ICMPv6 packets to disable the transmission of ICMPv6 Port Unreachable message.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Example

Enable GE 1/0/0 to send ICMPv6 Port Unreachable messages.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 icmp port-unreachable send
```

8.8.32 ipv6 icmp hop-limit-exceeded send

Function

The **ipv6 icmp hop-limit-exceeded send** command enables an interface to send ICMPv6 Hop Limit Exceeded messages.

 Copyright © Huawei Technologies Co., Ltd.

The **undo ipv6 icmp hop-limit-exceeded send** command disables the function.

By default, the enabling status of the function that the interface sends ICMPv6 Hop Limit Exceeded messages is the same as that of the function that the system sends ICMPv6 Hop Limit Exceeded messages.

Format

ipv6 icmp hop-limit-exceeded send

undo ipv6 icmp hop-limit-exceeded send

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

If a router receives a packet with a hop limit of 1, it replies with an ICMPv6 Hop Limit Exceeded message. This ICMPv6 error message carries the IPv6 address of the router as its source IPv6 address, which exposes the IPv6 address of the router and brings security risks. If the router is attacked by flooding packets, the router keeps replying with ICMPv6 Hop Limit Exceeded messages, causing high CPU usage and affecting device performance. To address this problem, run the **undo ipv6 icmp hop-limit-exceeded send** command on the inbound interface of ICMPv6 packets to disable the transmission of ICMPv6 Hop Limit Exceeded messages.

Example

Disable GE 1/0/0 from sending ICMPv6 Hop Limit Exceeded messages.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] undo ipv6 icmp hop-limit-exceeded send
```

8.8.33 ipv6 icmp receive

Function

The **ipv6 icmp receive** command enables the system to receive ICMPv6 packets.

The **undo ipv6 icmp receive** command disables the system from receiving ICMPv6 packets.

By default, the system receives ICMPv6 packets.

 Copyright © Huawei Technologies Co., Ltd.

Format

ipv6 icmp { *icmpv6-type icmpv6-code* | *icmpv6-name* | **all** } **receive**

undo ipv6 icmp { *icmpv6-type icmpv6-code* | *icmpv6-name* | **all** } **receive**

Parameters

Parameter	Description	Value
icmpv6-type	Specifies the type of ICMPv6 packets.	The value is an integer that ranges from 0 to 255.
icmpv6-code	Specifies the code of ICMPv6 packets.	The value is an integer that ranges from 0 to 255.
icmpv6-name	Specifies the name of ICMPv6 packets.	ICMPv6 packets are classified into the following types: • echo: Echo packet • echo-reply: Echo Reply packet • err-header-field: Packet with an error header • frag-time-exceeded: Fragmentation Timeout packet • hop-limit-exceeded: Packet whose hop count exceeds the limit • host-admin-prohib: Packet that is rejected by a host • host-unreachable: ICMPv6 Host Unreachable packet • neighbor-advertisement: Neighbor Advertisement packet • neighbor-solicitation: Neighbor Solicitation packet • network-unreachable: ICMPv6 Network Unreachable packet • packet-too-big: Packet Too Big packet • port-unreachable: ICMPv6 Port Unreachable packet • redirect: Redirected packets • router-advertisement: Router Advertisement packet • router-solicitation: Router Solicitation packet • unknown-ipv6-opt: Error packet with unknown options • unknown-next-hdr: Error packet with unknown next header

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all	Indicates all ICMPv6 packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the network is in good performance, devices can receive a proper number of ICMPv6 packets. However, when network traffic load is heavy, host unreachable or port unreachable events frequently occur, the devices receive a large number of ICMPv6 packets, which burdens the network and degrades device performance. In addition, attackers may use ICMPv6 error packets to probe the internal network topology.

To improve network performance and security, run the **undo ipv6 icmp receive** command to disable the system from receiving ICMPv6 Echo Reply packets, Host Unreachable packets, and Port Unreachable packets.

Precautions

When the network is in good performance again, you can run the **ipv6 icmp receive** command to enable the system to receive ICMPv6 packets.

After the **undo ipv6 icmp receive** command is run, a main interface is disabled from processing ICMPv6 packets, and the system does not collect statistics about ICMP Echo Reply packets, Host Unreachable packets, and Port Unreachable packets. Only statistics about discarded packets are collected.

Example

Disable the system from receiving ICMPv6 Echo packets.

```
<Huawei> system-view
[Huawei] undo ipv6 icmp echo receive
```

8.8.34 ipv6 icmp send

Function

The **ipv6 icmp send** command enables the system to send ICMPv6 packets.

The **undo ipv6 icmp send** command disables the system from sending ICMPv6 packets.

By default, the system is enabled to send ICMPv6 packets.

Copyright © Huawei Technologies Co., Ltd.

Format

ipv6 icmp { *icmpv6-type icmpv6-code* | *icmpv6-name* | **all** } **send**

undo ipv6 icmp { *icmpv6-type icmpv6-code* | *icmpv6-name* | **all** } **send**

Parameters

Parameter	Description	Value
icmpv6-type	Specifies the type of ICMPv6 packets.	The value is an integer that ranges from 0 to 255.
icmpv6-code	Specifies the code of ICMPv6 packets.	The value is an integer that ranges from 0 to 255.
icmpv6-name	Specifies the name of ICMPv6 packets.	ICMPv6 packets are classified into the following types: • echo: Echo packet • echo-reply: Echo Reply packet • err-header-field: Packet with an error header • frag-time-exceeded: Fragmentation Timeout packet • hop-limit-exceeded: Packet whose hop count exceeds the limit • host-admin-prohib: Packet that is rejected by a host • host-unreachable: ICMPv6 Host Unreachable packet • neighbor-advertisement: Neighbor Advertisement packet • neighbor-solicitation: Neighbor Solicitation packet • network-unreachable: ICMPv6 Network Unreachable packet • packet-too-big: Packet Too Big packet • port-unreachable: ICMPv6 Port Unreachable packet • redirect: ICMPv6 redirect message. • router-advertisement: Router Advertisement packet • router-solicitation: Router Solicitation packet • unknown-ipv6-opt: Error packet with unknown options • unknown-next-hdr: Error packet with unknown next header

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all	Indicates all ICMPv6 packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the network is in good performance, routing devices can send or receive ICMPv6 packets. However, when network traffic load is heavy, host unreachable or port unreachable events frequently occur, the routing devices send a large number of ICMPv6 packets, which burdens the network and degrades the performance of the routing devices. In addition, attackers may use ICMPv6 error packets to probe the internal network topology.

To improve network performance and security, run the **undo ipv6 icmp send** command to disable the system from sending ICMPv6 packets.

Precautions

When the network is in good performance again, you can run the **ipv6 icmp send** command to enable the system to send ICMPv6 packets.

Example

Disable the system from sending all ICMPv6 packets packets.

```
<Huawei> system-view
[Huawei] undo ipv6 icmp all send
```

8.8.35 ipv6 icmp too-big-rate-limit

Function

The **ipv6 icmp too-big-rate-limit** command enables a device to limit oversized ICMPv6 error packets.

The **undo ipv6 icmp too-big-rate-limit** command disables a device from limiting oversized ICMPv6 error packets.

By default, a device limit oversized ICMPv6 error packets.

Format

ipv6 icmp too-big-rate-limit

undo ipv6 icmp too-big-rate-limit

Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a host sends a large number of packets in a path with a small MTU, it may receive a large number of ICMPv6 error packets, affecting the processing of valid packets. This command limits the number of ICMPv6 error packets, ensuring host performance.

Example

Enable the device to limit oversized ICMPv6 error packets.

```
<Huawei> system-view
[Huawei] ipv6 icmp too-big-rate-limit
```

8.8.36 ipv6 mtu

Function

The **ipv6 mtu** command sets the MTU on the interface for sending IPv6 packets.

The **undo ipv6 mtu** command restores the default MTU of IPv6 packets on an interface.

By default, the MTU of IPv6 packets on an interface is 1500 bytes.

NOTE

- For the AR100 series, AR120 series, AR161, AR161W, AR161EW, AR161EW-M1, AR161G-L, AR161G-Lc, AR161G-U, AR169, AR169W, AR169EW, AR169EGW-L, AR169CVW, AR169CVW-4B4S, AR169G-L, AR169-P-M9, AR169W-P-M9, AR169RW-P-M9, the default value on the tunnel interface of the IPv6 over IPv4 tunnel is 1480 bytes.

Format

ipv6 mtu *mtu*

undo ipv6 mtu

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
mtu	Specifies the MTU value.	The value is an integer. The value of VE, VT, Dialer, GE, XGE, and Eth interfaces ranges from 1280 to 1610. The value of Eth, XGE sub-interfaces and GE sub-interfaces ranges from 1280 to 1606. The value of G.SHDSL and VDSL interfaces in the PTM mode ranges from 1280 to 1576. The value of PON, Async, Serial, POS, Cellular, Tunnel, VLANIF, Mp-group, and Eth-Trunk interfaces ranges from 1280 to 1500, in bytes. The default value is 1500.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

After the MTU value is changed using this command, run the **shutdown** and **undo shutdown** or **5.1.14 restart (interface view)** commands to restart the interface to make the changed MTU take effect.

It is recommended that the MTU of IPv6 packets on an interface should not exceed the MTU of IPv4 packets on an interface. (You can run the **mtu** command to configure the MTU of IPv4 packets on an interface.)

NOTE

- When deploying PPPoE services through VT or the dialer interface, you are advised to configure the IPv6 MTU on an interface smaller than 1568.
- When deploying MPoE services through VT or the dialer interface, you are advised to configure the IPv6 MTU on an interface smaller than 1572.

Example

Set the MTU of IPv6 packets on GE1/0/0 to 1280 bytes.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 mtu 1280
```

8.8.37 ipv6 nd autoconfig managed-address-flag

Function

The **ipv6 nd autoconfig managed-address-flag** command sets the M flag of stateful autoconfiguration in an RA packet.

Copyright © Huawei Technologies Co., Ltd.

The **undo ipv6 nd autoconfig managed-address-flag** command deletes the M flag of stateful autoconfiguration in an RA packet.

By default, the "managed address configuration" flag (M flag) is not set in the RA message.

Format

ipv6 nd autoconfig managed-address-flag

undo ipv6 nd autoconfig managed-address-flag

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- If the M flag is set, a host obtains an IPv6 address through stateful autoconfiguration.
- If the M flag is not set, a host uses stateless autoconfiguration to obtain an IPv6 address, that is, the host generates an IPv6 address based on the prefix information in the RA packet.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

The **ipv6 nd autoconfig managed-address-flag** command applies to GE interfaces and sub-interfaces, XGE interfaces and XGE sub-interfaces, Eth-Trunk interfaces and sub-interfaces, POS interfaces (only POS interfaces enabled with PPP or HDLC support the IPv6 function), and tunnel interfaces.

After the **ipv6 nd autoconfig managed-address-flag** command is run, a host can obtain configurations (excluding an IPv6 address) such as the router lifetime, neighbor reachable time, retransmission interval, and PMTU by means of stateful autoconfiguration even if the **ipv6 nd autoconfig other-flag** command is not run.

After the **display ipv6 interface** command is run, the command output shows that the attached hosts obtain IPv6 addresses through stateful autoconfiguration or stateless autoconfiguration.

The interface on the device cannot use stateful address autoconfiguration and stateless address autoconfiguration simultaneously to obtain IPv6 addresses.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the M flag of stateful autoconfiguration on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 nd autoconfig managed-address-flag
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.38 ipv6 nd autoconfig other-flag

Function

The **ipv6 nd autoconfig other-flag** command sets the "other configuration" flag (O flag) of stateful autoconfiguration in an RA packet.

The **undo ipv6 nd autoconfig other-flag** command deletes the O flag of stateful autoconfiguration in an RA packet.

By default, the O flag is not set in the RA packet.

Format

ipv6 nd autoconfig other-flag

undo ipv6 nd autoconfig other-flag

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- If the O flag is set, a host uses stateful autoconfiguration to obtain other configuration parameters (excluding an IPv6 address), including the router lifetime, neighbor reachable time, retransmission interval, and PMTU.
- If the O flag is not set, a host uses stateless autoconfiguration to obtain other configuration parameters, including the router lifetime, neighbor reachable time, retransmission interval, and PMTU. That is, the host obtains other configuration parameters through the RA packet advertised by routers.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

The **ipv6 nd autoconfig other-flag** command applies to GE interfaces and sub-interfaces, XGE interfaces and XGE sub-interfaces, Eth-Trunk interfaces and sub-interfaces, POS interfaces (only POS interfaces enabled with PPP or HDLC support the IPv6 function), and tunnel interfaces.

After the **ipv6 nd autoconfig managed-address-flag** command is run, a host can obtain other configurations (excluding IPv6 addresses) using stateful autoconfiguration even if the **ipv6 nd autoconfig other-flag** command is not run.

The interface on the device cannot use stateful autoconfiguration and stateless autoconfiguration simultaneously to obtain other configuration parameters excluding IPv6 addresses.

Example

Set the O flag of stateful autoconfiguration on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 nd autoconfig other-flag
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.39 ipv6 nd dad attempts

Function

The **ipv6 nd dad attempts** command sets the number of times NS packets are sent when the system performs Duplicate Address Detection (DAD).

The **undo ipv6 nd dad attempts** command restores the default value.

By default, the number of times NS packets are sent when the system performs DAD is 1.

Format

ipv6 nd dad attempts *value*

undo ipv6 nd dad attempts

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
value	Specifies the number of times NS packets are sent when the system performs DAD.	The value is an integer that ranges from 0 to 600. The default value is 1, which is recommended.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you configure an IPv6 address (a global unicast address or a link-local address) for an interface, check whether other interfaces connected to this interface have used the IPv6 address to be configured to prevent address conflicts.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

The **ipv6 nd dad attempts** command applies to the following interfaces: Ethernet interfaces and sub-interfaces, GE interfaces and sub-interfaces, serial interfaces (only serial interfaces enabled with PPP or HDLC support the IPv6 function), VT interfaces, VE interfaces, Eth-Trunk interfaces and sub-interfaces, VLANIF interfaces, and tunnel interfaces.

If the number of times NS packets are sent when the system performs DAD is set 0, DAD is prohibited.

If the physical link connected to an interface fails, DAD cannot be performed on the interface.

Example

Set the number of times NS packets are sent when the system performs DAD to 20 on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 nd dad attempts 20
```

Related Topics

8.8.28 ipv6 enable (interface view)

Copyright © Huawei Technologies Co., Ltd.

8.8.40 ipv6 nd hop-limit

Function

The **ipv6 nd hop-limit** command sets hop limit for IPv6 unicast packets initially sent by a device.

The **undo ipv6 nd hop-limit** command restores the hop limit for IPv6 unicast packets to the default value.

By default, the IPv6 unicast packets initially sent by a routing device can travel 64 hops.

Format

ipv6 nd hop-limit *limit*

undo ipv6 nd hop-limit

Parameters

Parameter	Description	Value
limit	Specifies the hop limit.	The value is an integer that ranges from 1 to 255. The default value is 64, which is recommended.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A hop limit on a device provides the following functions:

- Limiting the number of hops through which IPv6 unicast packets are allowed to travel.
- Functioning as a parameter in an RA packet to help a host automatically configure a hop limit (a limit on the number of hops through which IPv6 unicast packets initially sent by a host are allowed to travel).

Precautions

The hop limit for unicast packets is set using the **ipv6 nd hop-limit** command in the system view.

The hop limit for RA packets depends on the configuration of the **ipv6 nd hop-limit** command in the system view and the configuration of the **ipv6 nd ra hop-limit** command in the interface view.

Copyright © Huawei Technologies Co., Ltd.

- If the hop limit for RA packets is not set in the interface view or in the system view, the hop limit for RA packets is 64 by default.
- If the hop limit for RA packets is not set in the interface view, the value set using the **ipv6 nd hop-limit** command in the system view is used as the hop limit for RA packets.
- If the **ipv6 nd ra hop-limit** command is run in the interface view, the configuration in the interface view takes effect, no matter whether the hop limit is set in the system view.

The hop limit set for IPv6 unicast packets is the same as that set for RA packets. In the following cases, however, the hop limit for IPv6 unicast packets is 64, while the hop limit for RA packets is 0.

- No hop limit is set for IPv6 unicast packets. The default value takes effect.
- The **undo ipv6 nd hop-limit** command is run to restore the default hop limit set for IPv6 unicast packets.

After a host receives an RA packet with the hop limit of 0, it sets its hop limit to the default value 64, consistent with the default hop limit on the device.

Example

Set the hop limit for IPv6 unicast packets initially sent by a device to 100 in the system view.

```
<Huawei> system-view
[Huawei] ipv6 nd hop-limit 100
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.41 ipv6 nd learning strict

Function

The **ipv6 nd learning strict** command enables IPv6 neighbor discovery (ND) strict learning.

The **undo ipv6 nd learning strict** command disables IPv6 ND strict learning.

By default, IPv6 ND strict learning is disabled.

Format

In the system view:

ipv6 nd learning strict

undo ipv6 nd learning strict

In the interface view:

ipv6 nd learning strict { **force-disable** | **force-enable** | **trust** }

undo ipv6 nd learning strict

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
force-disable	Disables IPv6 ND strict learning forcibly.	-
force-enable	Enables IPv6 ND strict learning forcibly.	-
trust	Inherits the global setting of IPv6 ND strict learning.	-

Views

VLANIF interface view, Eth-trunk interface view, Eth-Trunk sub-interface view, system view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device uses neighbor advertisement (NA) packets to establish neighbor entries, which does not comply with RFC. To comply with RFC 4861, run the **ipv6 nd learning strict** command to enable IPv6 ND strict learning. After you enable IPv6 ND strict learning on a device, the device uses NA packets only in response to neighbor solicitation (NS) packets to establish neighbor entries.

The **ipv6 nd learning strict** and **undo ipv6 nd learning strict** commands apply only to VLANIF interfaces, Eth-Trunk interfaces, and Eth-Trunk sub-interfaces.

Precautions

Before running this command in an Eth-Trunk view, run the **undo portswitch** command to switch the Eth-Trunk to a Layer 3 interface.

After you run the **ipv6 nd learning strict** command on a device, the device synchronizes fake entries. Synchronizing a large number of fake entries affects device performance. Therefore, you are advised to use the command only for protocol consistency tests.

Example

Enable IPv6 ND strict learning globally.

```
<Huawei> system-view
[Huawei] ipv6 nd learning strict
```

Enable IPv6 ND strict learning on VLANIF 100 forcibly.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface vlanif 100
[Huawei-Vlanif100] ipv6 enable
[Huawei-Vlanif100] ipv6 nd learning strict force-enable
```

 Copyright © Huawei Technologies Co., Ltd.

8.8.42 ipv6 nd neighbor-limit

Function

The **ipv6 nd neighbor-limit** command configures the maximum number of dynamic neighbor entries that can be learned by an interface.

The **undo ipv6 nd neighbor-limit** command restores the default maximum number of dynamic neighbor entries that can be learned by an interface.

By default, an interface can learn a maximum of 1024 dynamic neighbor entries.

Format

ipv6 nd neighbor-limit *limit-number*

undo ipv6 nd neighbor-limit

Parameters

Parameter	Description	Value
limit-number	The maximum number of dynamic neighbor entries that can be learned by a specified interface.	The value is an integer in the range 2 to 4000.

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an interface learns too many neighbor entries, the processing load for the device will be increased and the performance of the device will be degraded. You can run the **ipv6 nd neighbor-limit** command to configure the maximum number of dynamic neighbor entries that can be learned by a specified interface.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command.

Example

Set the maximum number of dynamic neighbor entries that can be learned by the VLANIF100 interface to 10.

```
<Huawei> system-view
[Huawei] ipv6
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] interface vlanif 100
[Huawei-Vlanif100] ipv6 enable
[Huawei-Vlanif100] ipv6 nd neighbor-limit 10
```

8.8.43 ipv6 nd ns multicast-enable

Function

The **ipv6 nd ns multicast-enable** command enables a QinQ or a dot1q termination sub-interface to send NS multicast packets.

The **undo ipv6 nd ns multicast-enable** command disables a QinQ or a dot1q termination sub-interface from sending NS multicast packets.

By default, a QinQ or a dot1q termination sub-interface is disabled from sending NS multicast packets.

Format

ipv6 nd ns multicast-enable

undo ipv6 nd ns multicast-enable

Parameters

None

Views

Ethernet sub-interface view, GE sub-interface view, Eth-Trunk sub-interface view, XGE sub-interfaces

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A QinQ or a dot1q termination sub-interface on a routing device can send NS multicast packets to actively learn ND entries or respond to NS packets to passively learn ND entries.

When a QinQ or a dot1q termination sub-interface needs to send multicast NS packets to learn ND entries but there is no corresponding ND entry, you need to run this command to enable a QinQ or a dot1q termination sub-interface to send NS multicast packets.

Precautions

- If this command is not run on the termination sub-interface, the system discards the NS multicast packets.
- If this command is run on the termination sub-interface, the system tags an NS multicast packet and forwards it through the termination sub-interface.

 Copyright © Huawei Technologies Co., Ltd.

Sending multicast NS packets consumes CPU resources. Therefore, when the CPU performance of the system is rather low, you are advised not to enable a termination sub-interface to send NS multicast packets to actively learn ND entries but to respond to NS packets to passively learn ND entries.

Example

Enable the QinQ termination sub-interface GE2/0/0.1 to send NS multicast packets.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 2/0/0.1
[Huawei-GigabitEthernet2/0/0.1] qinq termination pe-vid 100 ce-vid 10
[Huawei-GigabitEthernet2/0/0.1] ipv6 enable
[Huawei-GigabitEthernet2/0/0.1] ipv6 nd ns multicast-enable
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.44 ipv6 nd ns retrans-timer

Function

The **ipv6 nd ns retrans-timer** command sets the interval for sending NS packets.

The **undo ipv6 nd ns retrans-timer** command restores the interval for sending NS packets to the default value.

By default, the interval for sending NS packets is 1000 ms.

Format

ipv6 nd ns retrans-timer *interval*

undo ipv6 nd ns retrans-timer

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending NS packets.	The value is an integer that ranges from 1000 to 4294967295, in milliseconds. The default value is 1000 milliseconds, which is recommended.

Views

Interface view

Default Level

2: Configuration level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

Setting the interval for sending NS packets provides the following functions:

- Controlling the interval at which a local routing device detects neighbor reachability.
- Controlling the interval at which a local routing device performs DAD.
- Functioning as a parameter in an RA packet to instruct hosts to specify this interval as their own interval for sending NS packets.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

The **ipv6 nd ns retrans-timer** command applies to GE interfaces and sub-interfaces, XGE interfaces and XGE sub-interfaces, Eth-Trunk interfaces and sub-interfaces, POS interfaces, and tunnel interfaces.

Frequently sending NS packets causes high CPU usage, which affects the system performance. Therefore, you are advised to set the interval for sending NS packets to a larger value. The default interval, 1000 milliseconds, is recommended.

If you run the **ipv6 nd ns retrans-timer** command multiple times, only the latest configuration takes effect.

The interval for sending NS packets is the same as that for sending RA packets. In the following cases, however, the interval for sending NS packets is the default value1000 ms, while the interval for sending RA packets is 0 ms.

- No interval for sending NS packets is set. The default value takes effect.
- The **undo ipv6 nd ns retrans-timer** command is run to restore the interval for sending NS packets to the default value.

After a host receives an RA packet of which the sending interval is 0 ms from a device, the host sets the interval for sending NS packet to 1000 ms, the same as that on the device.

Example

Set the interval for sending NS packets to 10000 milliseconds on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 nd ns retrans-timer 10000
```

Related Topics

8.8.28 ipv6 enable (interface view)

Copyright © Huawei Technologies Co., Ltd.

8.8.45 ipv6 nd nud reachable-time

Function

The **ipv6 nd nud reachable-time** command sets the IPv6 neighbor reachable time.

The **undo ipv6 nd nud reachable-time** command restores the IPv6 neighbor reachable time to the default value.

By default, the IPv6 neighbor reachable time is 1200000 ms.

Format

ipv6 nd nud reachable-time *value*

undo ipv6 nd nud reachable-time

Parameters

Parameter	Description	Value
value	Specifies the IPv6 neighbor reachable time.	The value is an integer that ranges from 1 to 3600000, in milliseconds. The default value is 1200000 ms, which is recommended.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Setting the IPv6 neighbor reachable time provides the following functions:

- Controlling the aging time of neighbor entries on a local routing device.
- Being a parameter in an RA packet to enable a host to configure the neighbor reachable time.

Each RA packet sent by a routing device carries the neighbor reachable time. This allows all nodes along the same link to use the same neighbor reachable time.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

A shorter neighbor reachable time enables a routing device to detect neighbor reachability more quickly. However, this consumes more network bandwidth and

Copyright © Huawei Technologies Co., Ltd.

CPU resources. Therefore, a short neighbor reachable time is not recommended on an IPv6 network. The default value, 1200000 ms, is recommended.

If you run the **ipv6 nd nud reachable-time** command multiple times, only the latest configuration takes effect.

The **ipv6 nd nud reachable-time** command applies to GE interfaces and sub-interfaces, XGE interfaces and XGE sub-interfaces, Eth-Trunk interfaces and sub-interfaces, POS interfaces (only POS interfaces enabled with PPP or HDLC support the IPv6 function), and tunnel interfaces.

The neighbor reachable time set on a routing device is the same as that carried in an RA packet. In the following cases, however, the neighbor reachable time set on a routing device is the default value 1200000 ms while the neighbor reachable time carried in the RA packet is 0 millisecond:

- No neighbor reachable time is set on the routing device. The default value takes effect.
- The **undo ipv6 nd nud reachable-time** command is run to restore the neighbor reachable time to the default value.

After a host receives an RA packet in which the neighbor reachable time is 0 ms, the host sets the neighbor reachable time to 1200000 ms, the same as that on the device.

Example

Set the neighbor reachable time to 10000 ms on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 nd nud reachable-time 10000
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.46 ipv6 nd ra

Function

The **ipv6 nd ra** command sets the interval for sending Router Advertisement packets.

The **undo ipv6 nd ra** command restores the interval for sending RA packets to the default value.

By default, the maximum interval is 600s and the minimum interval is 200s.

Format

ipv6 nd ra { **max-interval** *maximum-interval* | **min-interval** *minimum-interval* }

undo ipv6 nd ra { **max-interval** | **min-interval** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
max-interval *maximum-interval*	Specifies the maximum interval for sending RA packets.	The value is an integer that ranges from 4 to 1800, in seconds. The default value is 600 seconds, which is recommended. The maximum interval cannot be less than the minimum interval.
min-interval *minimum-interval*	Specifies the minimum interval for sending RA packets.	The value is an integer that ranges from 3 to 1350, in seconds. The default value is 200 seconds, which is recommended.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A routing device periodically sends RA packets. An RA packet carries both the IPv6 address prefix and the flag of stateful address autoconfiguration.

You can run the **ipv6 nd ra** command to change the interval for sending RA packets.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

Running the **ipv6 nd ra** command changes the interval for sending RA packets during DAD. Therefore, you are advised to use the default interval, that is, the maximum value is 600s and the minimum value is 200s.

If the **ipv6 nd ra** command is run multiple times, the latest configuration takes effect.

The **ipv6 nd ra** command applies to GE interfaces and sub-interfaces, XGE interfaces and XGE sub-interfaces, Eth-Trunk interfaces and sub-interfaces, POS interfaces (only POS interfaces enabled with PPP or HDLC support the IPv6 function), and tunnel interfaces.

The interval for sending RA packets cannot be longer than the lifetime of the RA packets. The default lifetime of the RA packets is 1800s and, you can run the **ipv6 nd ra router-lifetime** command to change the value.

Copyright © Huawei Technologies Co., Ltd.

The actual interval for sending RA packets is a random value between *min-interval* and *max-interval*.

Example

Set the maximum interval for sending RA packets to 1000s on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 nd ra max-interval 1000
```

Set the minimum interval for sending RA packets to 300s on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 nd ra min-interval 300
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.47 ipv6 nd ra halt

Function

The **ipv6 nd ra halt** command disables the system from sending RA packets.

The **undo ipv6 nd ra halt** command enables the system to send RA packets.

By default, the system is disabled from sending RA packets.

Format

ipv6 nd ra halt

undo ipv6 nd ra halt

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

- When a device is connected to a host, it periodically sends RA packets to the host. An RA packet carries the IPv6 address prefix and flag information of stateful autoconfiguration. You can run the **undo ipv6 nd ra halt** command to enable the device to send RA packets.
- When a device is connected to another device, that is, there is no host on the network, sending RA packets is not required. The default configuration is recommended.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

After the **ipv6 nd ra halt** command is run, the device does not send RA packets. In such a case, the hosts on the network cannot periodically receive information about updated IPv6 prefixes.

The **ipv6 nd ra halt** command applies to GE interfaces and sub-interfaces, XGE interfaces and XGE sub-interfaces, Eth-Trunk interfaces and sub-interfaces, POS interfaces, and tunnel interfaces.

By default, the device is disabled from sending RA packets. You can run the **display icmpv6 statistics** command to check whether a local device has sent RA packets.

Example

Disable GE1/0/0 from sending RA packets.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 nd ra halt
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.48 ipv6 nd ra hop-limit

Function

The **ipv6 nd ra hop-limit** command sets the hop limit for RA packets.

The **undo ipv6 nd ra hop-limit** command restores the hop limit for RA packets to the default value.

By default, the hop limit for RA packets is 64.

Format

ipv6 nd ra hop-limit *limit*

undo ipv6 nd ra hop-limit

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
limit	Specifies the hop limit for RA packets.	The value is an integer that ranges from 0 to 255. The default value is 64, which is recommended.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As a parameter in an RA packet, the hop limit enables a host to automatically configure a hop limit (a limit on the number of hops through which IPv6 unicast packets initially sent by a host are allowed to travel).

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

After this command is run on the router, the device discards the RA packet whose hop limit is different from its configuration.

- If the **ipv6 nd ra hop-limit** command is run on an interface, the hop limit for RA packets is determined by the interface configuration.
- If the **ipv6 nd ra hop-limit** command is not run on an interface, the hop limit for RA packets is determined by the hop limit configured using the **ipv6 nd hop-limit** command.

Example

Set the hop limit for RA packets sent by GE1/0/0 to 126.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 nd ra hop-limit 126
```

8.8.49 ipv6 nd ra preference

Function

The **ipv6 nd ra preference** command sets the priority of the default router in an RA packet.

Copyright © Huawei Technologies Co., Ltd.

The **undo ipv6 nd ra preference** command restores the priority of the default router in an RA packet to the default value.

By default, the priority of the default router in an RA packet is medium.

Format

ipv6 nd ra preference { **high** | **medium** | **low** }

undo ipv6 nd ra preference

Parameters

Parameter	Description	Value
high	Sets the default router priority to high.	-
medium	Sets the default router priority to medium.	-
low	Sets the default router priority to low.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple routers exist on the link where a host resides, the host chooses the forwarding router based on the destination address of the packet. Each router sends an RA packet that contains the default router priority and route information to the host, which helps the host choose the proper router based on the destination address.

The host updates its routing table after receiving the RA packet. To forward packets to other devices, the host checks the routing table to choose the proper route.

When the default router list of the host includes multiple entries, run this command to configure the router with the highest priority on the local link as the default router (gateway) of the host.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

By default, the router does not send RA packets. You need to run the **undo ipv6 nd ra halt** command to enable the router to send RA packets to the host.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

If the interface is being unbound from the VPN instance that has IPv6 address family enabled, the system displays a message, indicating that this command cannot be run.

Example

Set the priority of the default router in an RA packet to high on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] undo ipv6 nd ra halt
[Huawei-GigabitEthernet1/0/0] ipv6 nd ra preference high
```

Related Topics

8.8.28 ipv6 enable (interface view)
8.8.47 ipv6 nd ra halt
8.8.51 ipv6 nd ra route-information

8.8.50 ipv6 nd ra prefix

Function

The **ipv6 nd ra prefix** command configures the prefix in an RA packet.

The **undo ipv6 nd ra prefix** command deletes the prefix in an RA packet.

By default, an RA packet carries only the address prefix configured using the **ipv6 address** command.

Format

ipv6 nd ra prefix { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* } *valid-lifetime preferred-lifetime* [**no-autoconfig**] [**off-link**]

undo ipv6 nd ra prefix { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* }

ipv6 nd ra prefix default no-advertise

undo ipv6 nd ra prefix default no-advertise

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address carried in the RA packet.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
prefix-length	Specifies the prefix length of an IPv6 address.	The value is an integer that ranges from 1 to 128. You can calculate the IPv6 prefix carried in the RA packet based on the IPv6 address and prefix length.
valid-lifetime	Specifies the valid lifetime of the prefix.	The value is an integer that ranges from 0 to 4294967295, in seconds.
preferred-lifetime	Specifies the preferred lifetime of the prefix.	The value is an integer that ranges from 0 to 4294967295, in seconds. The preferred lifetime cannot be larger than the valid lifetime.
no-autoconfig	Deletes the A-Flag. If this parameter is configured, a configured prefix cannot be used in stateless address allocation.	-
off-link	Specifies the O-Flag. If **off-link** is specified, the prefix carried in the RA packet cannot be allocated to the local link. When the host sends a packet to the address specified by this prefix, the packet is forwarded through a default router.	-
default no-advertise	Specifies that RA packets do not carry the default prefix generated based on the interface IPv6 address.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable a routing device to advertise only a specified prefix, run the **ipv6 nd ra prefix** command to configure the prefix.

 Copyright © Huawei Technologies Co., Ltd.

If a prefix has been configured using the **ipv6 nd ra prefix** command, the device advertises both prefixes configured using the **ipv6 nd ra prefix** and **ipv6 address** commands.

By default, RA packets carry the default prefix generated based on the interface IPv6 address. If the default setting is not required, run the **ipv6 nd ra prefix default no-advertise** command.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

After a host receives the RA packet with the prefix configured using the **ipv6 nd ra prefix** command, the host updates the local prefix information.

The **ipv6 nd ra prefix** command applies to the following interfaces: GE interfaces and sub-interfaces, Eth-Trunk interfaces and sub-interfaces, POS interfaces (only POS interfaces enabled with PPP or HDLC support the IPv6 function), and tunnel interfaces.

The prefix configured using the **ipv6 nd ra prefix** command cannot be fe80:: (prefix of a link-local address), ff00:: (prefix of a multicast address), :: (prefix of an unspecified address), or the prefix that has been used by another interface (including the interface address prefix and prefix carried in RA packets).

Example

Configure the prefix in the RA packet on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] undo ipv6 nd ra halt
[Huawei-GigabitEthernet1/0/0] ipv6 nd ra prefix fc00:1::100 128 1000 400 no-autoconfig
[Huawei-GigabitEthernet1/0/0] ipv6 nd ra prefix fc00:2::100 64 1000 400 off-link
```

Configure RA packets on GE1/0/0 not to carry the default prefix.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] undo ipv6 nd ra halt
[Huawei-GigabitEthernet1/0/0] ipv6 nd ra prefix default no-advertise
```

Related Topics

8.8.47 ipv6 nd ra halt

8.8.51 ipv6 nd ra route-information

Function

The **ipv6 nd ra route-information** command configures route option information in an RA packet.

Copyright © Huawei Technologies Co., Ltd.

The **undo ipv6 nd ra route-information** command deletes route option information in an RA packet.

By default, no route option information is configured in an RA packet.

Format

ipv6 nd ra route-information *ipv6-address prefix-length* **lifetime** *route-lifetime* [**preference** { **high** | **medium** | **low** }]

undo ipv6 nd ra route-information *ipv6-address prefix-length*

Parameters

Parameter	Description	Value
ipv6-address	Specifies the prefix of an IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
prefix-length	Specifies the prefix length of an IPv6 address.	The value is an integer that ranges from 0 to 128.
lifetime *route-lifetime*	Specifies the route lifetime.	The value is an integer that ranges from 0 to 4294967295, in seconds.
preference	Specifies the route priority.	-
high	Sets the route priority to high.	-
medium	Sets the route priority to medium.	-
low	Sets the route priority to low.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An RA packet contains route options. The router sends the specified routes to the hosts on the local network segment by using these route options. The hosts can send packets by using these routes.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

By default, the router does not send RA packets. You need to run the **undo ipv6 nd ra halt** command to enable the router to send RA packets to the host.

Precautions

The host updates its routing table after receiving the RA packet that carries route option information. To forward packets to other devices, the host checks the routing table to choose the proper route.

A maximum of 17 route options are supported on each interface.

Route option information cannot be configured for a loopback address.

Example

Configure route information of RA packets on GE1/0/0: setting the lifetime of the route with the destination address of FC00:1::1/64 to 1550s, and the priority of this route to high.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] undo ipv6 nd ra halt
[Huawei-GigabitEthernet1/0/0] ipv6 nd ra route-information fc00:1::1 64 lifetime 1550 preference high
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.47 ipv6 nd ra halt

8.8.49 ipv6 nd ra preference

8.8.52 ipv6 nd ra router-lifetime

Function

The **ipv6 nd ra router-lifetime** command sets the lifetime of RA packets.

The **undo ipv6 nd ra router-lifetime** command restores the lifetime of RA packets to the default value.

By default, the lifetime for RA messages is three times of the maximum interval for advertising RA messages.

Format

ipv6 nd ra router-lifetime *ra-lifetime*

undo ipv6 nd ra router-lifetime

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ra-lifetime	Specifies the lifetime of RA packets.	The value is an integer and can be 0 or ranges from 4 to 9000, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device adds the lifetime value to an RA packet before sending the RA packet to the host on the local network segment. The lifetime of RA packet indicates the time that a router functions as the default gateway for a host.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

If a host receives an RA packet with the lifetime field being 0, the host does not add the address of the router to its default router table.

The **ipv6 nd ra router-lifetime** command applies to GE interfaces and sub-interfaces, XGE interfaces and XGE sub-interfaces, Eth-Trunk interfaces and sub-interfaces, POS interfaces (only POS interfaces enabled with PPP or HDLC support the IPv6 function), and tunnel interfaces.

The lifetime of the RA packets cannot be smaller than the interval for sending RA packets. By default, the maximum interval for sending RA packets is 600s and the minimum interval is 200s. You can run the **ipv6 nd ra** command to set the interval. If the set lifetime value of the RA packets is smaller than the set interval for sending RA packets, the system displays an error. In such a case, you need to reset the lifetime value.

Example

Set the lifetime of the RA packets on GE1/0/0 to 1000s.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 nd ra router-lifetime 1000
```

Related Topics

8.8.28 ipv6 enable (interface view)

Copyright © Huawei Technologies Co., Ltd.

8.8.53 ipv6 nd stale-timeout

Function

The **ipv6 nd stale-timeout** command sets the aging time of ND entries in STALE state.

The **undo ipv6 nd stale-timeout** command restores the aging time of ND entries in STALE state to the default value.

By default, the aging time of ND entries in STALE state is 1200s in the system view and is not set in the interface view.

Format

ipv6 nd stale-timeout *timeout-value*

undo ipv6 nd stale-timeout

Parameters

Parameter	Description	Value
timeout-value	Specifies the aging time of ND entries in STALE state.	The value is an integer that ranges from 60 to 172800, in seconds. The default value is 1200s, which is recommended.

Views

System view and Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The STALE state of an ND entry indicates that whether the neighbor is reachable is unknown. A device does not detect the neighbor reachability unless packets need to be sent to a neighbor.

The aging time of ND entries in STALE state is configurable. To quickly clear invalid ND entries, set the aging time to a smaller value using the **ipv6 nd stale-timeout** command. This speeds up entry aging.

Prerequisites

The device is enabled to forward IPv6 packets using the **ipv6** command in the system view.

IPv6 has been enabled on the interface using the **ipv6 enable** command in the interface view.

Copyright © Huawei Technologies Co., Ltd.

Precautions

After the **ipv6 nd stale-timeout** command is run, the status of ND entries can be updated after the aging time of ND entries in STALE state expires.

The system checks the validity of ND entries after the aging time of ND entries in STALE state expires. If the neighbor is reachable, the ND entry status changes to REACH; otherwise, the ND entry is deleted.

When the aging time is not set on interfaces, the aging time set in the system is used. When the aging time is set on interfaces, the setting on the interfaces takes effect with priority.

Example

Set the aging time of ND entries in STALE state to 3600s on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 nd stale-timeout 3600
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.54 ipv6 neighbor

Function

The **ipv6 neighbor** command configures static neighbor entries.

The **undo ipv6 neighbor** command deletes static neighbor entries.

By default, no static neighbor entry is configured.

Format

ipv6 neighbor *ipv6-address mac-address*

ipv6 neighbor *ipv6-address mac-address* **vid** *vlan-id interface-type interface-number*

ipv6 neighbor *ipv6-address mac-address* **vid** *vlan-id* [**cevid** *cevid*]

undo ipv6 neighbor *ipv6-address*

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of a neighbor.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
mac-address	Specifies the MAC address of a static neighbor.	The value is a 48-digit number in H-H-H format.
vid *vlan-id*	Specifies the ID of the VLAN to which the VLANIF interface belongs.	The value is an integer that ranges from 1 to 4094.
cevid *cevid*	Specifies the inner VLAN ID.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Specifies the interface type and number of a physical interface.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **ipv6 neighbor** command applies to GE interfaces and sub-interfaces, XGE interfaces and XGE sub-interfaces, and Eth-Trunk interfaces and sub-interfaces. You can run the **ipv6 neighbor** command to configure the mapping between the IPv6 address and MAC address for a neighbor. A neighbor entry indicates the mapping between an IPv6 address and a MAC address.

To filter invalid packets, you can create static neighbor entries, binding the destination IPv6 addresses of these packets to nonexistent MAC addresses.

Run the following commands based on the interface type:

- To configure static neighbor entries for Layer 3 interfaces, run the **ipv6 neighbor** *ipv6-address mac-address* command.
- To configure static neighbor entries for VLANIF interfaces, run the **ipv6 neighbor** *ipv6-address mac-address* **vid** *vlan-id interface-type nterface-number* command.
- To configure static neighbor entries for QinQ termination sub-interfaces or a dot1q termination sub-interfaces, run the **ipv6 neighbor** *ipv6-address mac-address* **vid** *vlan-id* [**cevid** *cevid*] command.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

A neighbor entry enters the REACHABLE state after being created, indicating that the interface connected to this neighbor is Up. If the interface connected to this neighbor becomes Down, the neighbor entry needs to be deleted.

The static neighbor entries overwrite the neighbor entries dynamically learnt by device. That is, static neighbor entries are of higher priorities than dynamically learnt neighbor entries.

If the IPv6 address or MAC address specified in the **ipv6 neighbor** command is incorrect, communication with this neighbor fails.

Example

Configure static neighbor entries on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 neighbor fc00::1 0019-7459-3301
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.10 display ipv6 neighbors

8.8.55 ipv6 pathmtu

Function

The **ipv6 pathmtu** command sets the PMTU for a specified destination IPv6 address.

The **undo ipv6 pathmtu** command deletes the PMTU for a specified destination IPv6 address.

Format

ipv6 pathmtu *ipv6-address* [**vpn-instance** *vpn-instance-name*] [*path-mtu*]

undo ipv6 pathmtu *ipv6-address* [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address for which a PMTU is to be set.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
vpn-instance *vpn-instance-name*	Specifies the name of an IPv6 VPN instance for which a PMTU is to be set.	The value must be an existing VPN instance.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
path-mtu	Specifies the path MTU, that is, the maximum size of IPv6 packets allowed to be sent along the path.	The value is an integer that ranges from 1280 to 10000, in bytes. The default value is 1500, which is recommended.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A PMTU is used to determine the proper size of packets to be transmitted along the path from a source to a destination. Usually, a device fragments and forwards packets based on the dynamically learnt PMTU. Packets that are sent using this PMTU do not need to be fragmented during transmission. This reduces pressure on routing devices and optimizes network resource utilization to obtain the maximum throughput.

In some special cases, however, to protect devices on the network and avoid large-size packet attacks, you can run the **ipv6 pathmtu** command to set a static PMTU for the specified destination IPv6 address to control the maximum size of packets that can be transmitted between the source and the destination.

Precautions

On the path along which packets are transmitted, a node discards the received packets if its MTU is smaller than the PMTU of the received packets. Therefore, in most cases, dynamic PMTU learning is recommend unless there are security vulnerabilities on the network. You can use the default PMTU value instead of running the **ipv6 pathmtu** command to set a static PMTU.

Example

Set the PMTU of a specified IPv6 destination address to 1300 bytes.

```
<Huawei> system-view
[Huawei] ipv6 pathmtu fc00::12 1300
```

Set the PMTU of the address fc00::1 of the IPv6 VPN instance to 1600 bytes.

```
<Huawei> system-view
[Huawei] ipv6 pathmtu fc00::1 vpn-instance vpn6 1600
```

Related Topics

8.8.56 ipv6 pathmtu age

8.8.11 display ipv6 pathmtu

Copyright © Huawei Technologies Co., Ltd.

8.8.56 ipv6 pathmtu age

Function

The **ipv6 pathmtu age** command sets the aging time of dynamic PMTU entries.

The **undo ipv6 pathmtu age** command restores the aging time of dynamic PMTU entries to the default value.

By default, the aging time of dynamic PMTU entries is 10 minutes.

Format

ipv6 pathmtu age *age-time*

undo ipv6 pathmtu age

Parameters

Parameter	Description	Value
age-time	Specifies the aging time of dynamic specified PMTU entries.	The value is an integer that ranges from 10 to 100, in minutes. The default value is 10 minutes, which is recommended.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The lifetime of a dynamic PMTU entry can be changed by setting an aging time for dynamic PMTU entries.

To slow down PMTU aging, run the **ipv6 pathmtu age** command to set the aging time of dynamic PMTU entries to a larger value.

Precautions

This command changes only the aging time of dynamic PMTUs but not static PMTUs because static PMTU entries never age.

The priority of a static PMTU is higher than that of a dynamic PMTU. If the static PMTU exists, the dynamic PMTU does not take effect.

The aging time for the PMTU is valid only for the dynamic PMTU entries generated after this configuration, instead of the PMTU entries generated before this configuration.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the aging time of dynamic PMTU entries to 40 minutes.

```
<Huawei> system-view
[Huawei] ipv6 pathmtu age 40
```

Related Topics

8.8.55 ipv6 pathmtu

8.8.11 display ipv6 pathmtu

8.8.57 ipv6 soft-forward enhance enable

Function

The **ipv6 soft-forward enhance enable** command enables the enhanced forwarding function for IPv6 control packets generated by the device.

The **undo ipv6 soft-forward enhance enable** command disables the enhanced forwarding function for IPv6 control packets generated by the device.

By default, the enhanced forwarding function is enabled for IPv6 control packets generated by the device.

Format

ipv6 soft-forward enhance enable

undo ipv6 soft-forward enhance enable

Parameters

None.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure forwarding policies (such as QoS policies) for data packets to implement differentiated services. In some scenarios, you may need to manage control packets generated by the device to process different control packets. For example, carriers have limited the bandwidth of data packets through QoS policies and also want to limit the bandwidth of control packets. In this situation, QoS policies take effect only for data packets. You can configure the enhanced forwarding function to make QoS policies take effect for control packets. Currently, the enhanced forwarding function is valid only for the control packets

 Copyright © Huawei Technologies Co., Ltd.

generated by the device but not for the control packets forwarded by other devices.

You can run the **ipv6 soft-forward enhance enable** command to enable the enhanced forwarding function for IPv6 control packets generated by the device.

Follow-up Procedures

After enabling the enhanced forwarding function on the device, you can perform some configurations on the IPv6 control packets generated by the device. For example, you can configure different QoS policies for different types of IPv6 control packets generated by the device.

Example

Disable the enhanced forwarding function for IPv6 control packets generated by the device.

```
<Huawei> system-view
[Huawei] undo ipv6 soft-forward enhance enable
```

8.8.58 reset ipv6 address-policy

Function

The **reset ipv6 address-policy** command deletes policy entries for selecting addresses.

Format

reset ipv6 address-policy [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Deletes policy entries for selecting the address of a specified VPN instance. *vpn-instance-name* specifies the name of a VPN instance.	The value must be an existing VPN instance.

Views

User view

Default Level

3: Management level

Usage Guidelines

The **reset ipv6 address-policy** command deletes policy entries for selecting addresses. Therefore, confirm your action before running this command.

This command does not delete policy entries for selecting default addresses.

 Copyright © Huawei Technologies Co., Ltd.

Example

Delete policy entries for selecting addresses.

```
<Huawei> reset ipv6 address-policy
```

8.8.59 reset ipv6 attack-source overlapping-fragment

Function

The **reset ipv6 attack-source overlapping-fragment** command clears statistics on overlapping fragment attack packets.

Format

reset ipv6 attack-source overlapping-fragment

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

After overlapping fragment attack packets are processed manually, run the **reset ipv6 attack-source overlapping-fragment** command to clear statistics on overlapping fragment attack packets.

Example

Clear statistics on IPv6 overlapping fragment attack packets.

```
<Huawei> reset ipv6 attack-source overlapping-fragment
```

Related Topics

8.8.7 display ipv6 attack-source overlapping-fragment

8.8.60 reset ipv6 neighbors

Function

The **reset ipv6 neighbors** command clears neighbor entries.

 Copyright © Huawei Technologies Co., Ltd.

Format

reset ipv6 neighbors { **all** | **dynamic** | **static** | **vid** *vlan-id* [*interface-type interface-number*] | *interface-type interface-number* [**dynamic** | **static**] }

Parameters

Parameter	Description	Value
all	Clears neighbor entries on all interfaces.	-
dynamic	The first **dynamic** indicates that dynamic neighbor entries on all interfaces are cleared. The second **dynamic** indicates that dynamic neighbor entries on the current interface are cleared.	-
static	The first **static** indicates that static neighbor entries on all interfaces are cleared. The second **static** indicates that static neighbor entries on the current interface are deleted.	-
vid *vlan-id*	Clears neighbor entries of a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Clears all neighbor entries on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the number of neighbor entries exceeds the upper limit, run the **reset ipv6 neighbors** command to clear excessive neighbor entries.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

The **reset ipv6 neighbors** command clears specified neighbor entries, which affects IPv6 packet forwarding. Therefore, confirm your action before running this command.

Example

Clear all neighbor entries on all interfaces.

```
<Huawei> reset ipv6 neighbors all
Warning: This operation will delete all static and dynamic IPv6 ND entries and the configurations of all static IPv6 ND. Continue?[Y
/N]:y
```

Clear all neighbor entries on GE1/0/0.

```
<Huawei> reset ipv6 neighbors gigabitethernet 1/0/0
```

Related Topics

8.8.10 display ipv6 neighbors

8.8.61 reset ipv6 pathmtu

Function

The **reset ipv6 pathmtu** command clears PMTU entries.

Format

reset ipv6 pathmtu [**vpn-instance** *vpn-instance-name*] { **all** | **dynamic** | **static** }

Parameters

Parameter	Description	Value
all	Clears all PMTU entries in the cache.	-
dynamic	Clears all dynamic PMTU entries in the cache.	-
static	Clears all static PMTU entries in the cache.	-
vpn-instance *vpn-instance-name*	Clears all PMTU entries of a specified IPv6 VPN instance.	The value must be an existing VPN instance.

Views

User view

Default Level

3: Management level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The **reset ipv6 pathmtu** command clears all PMTU entries. Therefore, confirm your action before running this command.

Example

Clear all PMTU entries.

```
<Huawei> reset ipv6 pathmtu all
Warning: This operation will reset all static and dynamic IPv6 PMTU entries, and clear the configurations of all static IPv6 PMTU, c
ontinue?[Y/N]:y
```

Related Topics

8.8.55 ipv6 pathmtu

8.8.62 reset ipv6 socket pktsort

Function

The **reset ipv6 socket pktsort** command clears statistics on the dual receive buffer of an IPv6 socket.

Format

reset ipv6 socket pktsort task-id *task-id* **socket-id** *socket-id*

Parameters

Parameter	Description	Value
task-id *task-id*	Specifies the ID of a task.	The value is an integer that ranges from 1 to 350.
socket-id *socket-id*	Specifies the ID of a socket.	The value is an integer that ranges from 1 to 131072.

Views

User view

Default Level

3: Management level

Usage Guidelines

This command clears statistics on the dual receive buffer of an IPv6 socket and the count restarts. Therefore, confirm your action before running this command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Clear statistics on the dual receive buffer of the IPv6 socket with the task ID 2 and the socket ID 4.

```
<Huawei> reset ipv6 socket pktsort task-id 2 socket-id 4
```

8.8.63 reset ipv6 statistics

Function

The **reset ipv6 statistics** command clears IPv6 traffic statistics.

Format

reset ipv6 statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To collect IPv6 traffic statistics within a specified period, clear the existing IPv6 traffic statistics before running the **display ipv6 statistics** command to display IPv6 traffic statistics.

Precautions

The **reset ipv6 statistics** command clears the specified IPv6 traffic statistics. Therefore, confirm your action before running this command.

Example

Clear IPv6 traffic statistics.

```
<Huawei> reset ipv6 statistics
```

Related Topics

8.8.13 display ipv6 statistics

8.8.64 reset rawip ipv6 statistics

Function

The **reset rawip ipv6 statistics** command clears all Raw IPv6 packet statistics.

Format

reset rawip ipv6 statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

You need to run this command to clear the existing statistics on Raw IPv6 packets before running the **display rawip ipv6 statistics** command to view statistics on Raw IPv6 packets in a specified period.

The **reset rawip ipv6 statistics** command clears statistics on Raw IPv6 packets. Therefore, confirm your action before running this command.

Example

Clear all Raw IPv6 packet statistics.

```
<Huawei> reset rawip ipv6 statistics
```

8.8.65 reset tcp ipv6 authentication-statistics

Function

The **reset tcp ipv6 authentication-statistics** command clears authentication statistics of a specified TCP6 connection.

Format

reset tcp ipv6 authentication-statistics src-ip *src-ip* **src-port** *src-port* **dest-ip** *dest-ip* **dest-port** *dest-port*

Parameters

Parameter	Description	Value
src-ip *src-ip*	Specifies the source IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
src-port *src-port*	Specifies the source port.	The value is an integer that ranges from 0 to 65535.
dest-ip *dest-ip*	Specifies the destination IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
dest-port *dest-port*	Specifies the destination port.	The value is an integer that ranges from 0 to 65535.

Views

User view

Default Level

3: Management level

Usage Guidelines

The **reset tcp ipv6 authentication-statistics** command clears authentication statistics of a TCP6 connection. Therefore, confirm your action before running this command.

Example

Clear authentication statistics of a TCP6 connection.

```
<Huawei> reset tcp ipv6 authentication-statistics src-ip fc00:1::1 src-port 3456 dest-ip fc00:3::5 dest-port 5678
```

Related Topics

8.8.15 display tcp ipv6 authentication-statistics

8.8.66 reset tcp ipv6 statistics

Function

The **reset tcp ipv6 statistics** command clears IPv6 TCP packet statistics.

Format

reset tcp ipv6 statistics

Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You need to clear the existing statistics on IPv6 TCP packets before running the **display tcp ipv6 statistics** command to view the statistics on IPv6 TCP packets in a specified period.

Precautions

The **reset tcp ipv6 statistics** command clears statistics on IPv6 TCP packets. Therefore, confirm your action before running this command.

The **reset tcp ipv6 statistics** command clears IPv6 TCP packet statistics on all in-service interface boards.

Example

Clear IPv6 TCP packet statistics.

```
<Huawei> reset tcp ipv6 statistics
```

Related Topics

8.8.16 display tcp ipv6 statistics

8.8.67 reset udp ipv6 statistics

Function

The **reset udp ipv6 statistics** command clears IPv6 UDP packet statistics.

Format

reset udp ipv6 statistics

Parameters

None

Views

User view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You need to run this command to clear the existing IPv6 UDP packet statistics before running the **display udp ipv6 statistics** command to view IPv6 UDP packet statistics in a specified period.

Precautions

The **reset udp ipv6 statistics** command clears IPv6 UDP packet statistics. Therefore, confirm your action before running this command.

The **reset udp ipv6 statistics** command clears IPv6 UDP packet statistics on all in-service interface boards.

Example

Clear IPv6 UDP packet statistics.

```
<Huawei> reset udp ipv6 statistics
```

8.8.68 set priority acl6 dscp

Function

The **set priority acl6 dscp** command configures the DSCP priority of IPv6 control packets generated by the device based on the ACL rule.

The **undo set priority acl6** command restores the default DSCP priority of IPv6 control packets generated by the device.

By default, the DSCP priority of IPv6 control packets generated by the device is not specified based on the ACL rule.

Format

set priority acl6 *acl6-number* **dscp** *dscp-value*

undo set priority acl6 *acl6-number*

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of an ACL rule.	The value is an integer that ranges from 3000 to 3999.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
dscp-value	Specifies the DSCP priority of IPv6 control packets.	The value is as follows: • The value is an integer that ranges from 0 to 63. • The value can be **ef**, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, or **default**.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **8.8.57 ipv6 soft-forward enhance enable** command is executed to enable the enhanced forwarding function of IPv6 control packets generated by the device, the same QoS policy will be applied to both the control packets and data packets. When the device maps packets based on DSCP priorities, it may send some control packets with low DSCP priorities generated on the device to low-priority queues, such as ICMPv6 and IPv6 Telnet packets. You can run the **set priority acl6 dscp** command to configure the DSCP priority of IPv6 control packets generated by the device based on the ACL rule, to prevent these IPv6 control packets from entering low-priority queues.

Precautions

If you run the **set priority acl6 dscp** command with the same value of *acl6-number* multiple times, only the latest configuration takes effect.

You can run the **8.8.69 set priority protocol-type-ipv6 dscp** command to specify the DSCP priority of IPv6 control packets based on the protocol type. If you specify the DSCP priority of IPv6 control packets based on both the protocol type and ACL rule, the protocol type configuration takes effect preferentially.

If you specify the DSCP priority of IPv6 control packets based on the ACL rule, you can configure a maximum of 16 ACL rules.

Example

Set the DSCP priority of IPv6 control packets based on the ACL6 rule 3002 to 56.

Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] set priority acl6 3002 dscp 56
```

Related Topics

8.8.57 ipv6 soft-forward enhance enable

8.8.69 set priority protocol-type-ipv6 dscp

8.8.69 set priority protocol-type-ipv6 dscp

Function

The **set priority protocol-type-ipv6 dscp** command configures the DSCP priority of IPv6 control packets generated by the device based on the protocol type.

The **undo set priority protocol-type-ipv6 dscp** command restores the default DSCP priority of IPv6 control packets generated by the device.

By default, the DSCP priority of IPv6 control packets generated by the device is 0.

Format

set priority protocol-type-ipv6 *protocol-type* **dscp** *dscp-value*

undo set priority protocol-type-ipv6 *protocol-type* **dscp**

Parameters

Parameter	Description	Value
protocol-type	Specifies the DSCP priority based on the IPv6 protocol type.	Enumerated type. The value can be **bgp4plus**, **dns6**, **icmpv6**, **snmp**, **ssh**, **udp**, or **telnet**.
dscp-value	Specifies the DSCP priority of IPv6 control packets.	The value is as follows: • The value is an integer that ranges from 0 to 63. • The value can be **ef**, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, or **default**.

Views

System view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **8.8.57 ipv6 soft-forward enhance enable** command is executed to enable the enhanced forwarding function of IPv6 control packets generated by the device, the same QoS policy will be applied to both the control packets and data packets. When the device maps packets based on DSCP priorities, it may send some control packets with low DSCP priorities generated on the device to low-priority queues, such as ICMPv6 and IPv6 Telnet packets. You can run the **set priority protocol-type-ipv6 dscp** command to configure the DSCP priority of IPv6 control packets generated by the device based on the protocol type, to prevent these IPv6 control packets from entering low-priority queues.

Precautions

If you run the **set priority protocol-type-ipv6 dscp** command with the same value of **protocol-type-ipv6** multiple times, only the latest configuration takes effect.

To configure DSCP priorities of multiple IPv6 control packets, run the **set priority protocol-type-ipv6 dscp** command multiple times.

You can run the **8.8.68 set priority acl6 dscp** command to specify the DSCP priority of IPv6 control packets based on the ACL rule. If you specify the DSCP priority of IPv6 control packets based on both the protocol type and ACL rule, the protocol type configuration takes effect preferentially.

Example

Set the DSCP priority of IPv6 Telnet packets to 56.

```
<Huawei> system-view
[Huawei] set priority protocol-type-ipv6 telnet dscp 56
```

Related Topics

8.8.57 ipv6 soft-forward enhance enable

8.8.68 set priority acl6 dscp

8.8.70 tcp ipv6 max-mss

Function

The **tcp ipv6 max-mss** command sets the maximum value of Maximum Segment Size (MSS) for a TCP6 connection.

The **undo tcp ipv6 max-mss** command deletes the maximum MSS value of a TCP6 connection.

By default, the maximum MSS value is not configured for TCP6 connections.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

This function takes effect only for TCP6 packets transmitted over a TCP6 connection established with the local device.

Format

tcp ipv6 max-mss *mss-value*

undo tcp ipv6 max-mss

Parameters

Parameter	Description	Value
mss-value	Specifies the maximum MSS value for a TCP6 connection.	The value is an integer ranging from 32 to 9600, in bytes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To establish a TCP6 connection, the MSS value is negotiated, which indicates the maximum length of packets that the local device can receive. If the path MTU is unavailable on one end of a TCP6 connection, this end cannot adjust the TCP6 packet size based on the MTU. As a result, this end may send TCP6 packets that are longer than the MTUs on intermediate devices, which will discard these packets. To prevent this problem, run the **tcp ipv6 max-mss** command on either end of a TCP6 connection to set the maximum MSS value of TCP6 packets. Then the MSS value negotiated by both ends will not exceed this maximum MSS value, and accordingly TCP6 packets sent from both ends will not be longer than this maximum MSS value and can travel through the intermediate network.

Precautions

The maximum MSS value configured using the **tcp ipv6 max-mss** command must be greater than the minimum MSS value configured using the **tcp ipv6 min-mss** command.

Example

Set the maximum MSS value for a TCP6 connection to 1024 bytes.

```
<Huawei> system-view
[Huawei] tcp ipv6 max-mss 1024
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

8.8.71 tcp ipv6 min-mss

8.8.71 tcp ipv6 min-mss

Function

The **tcp ipv6 min-mss** command sets the minimum value of maximum segment size (MSS) for a TCP6 connection.

The **undo tcp ipv6 min-mss** command restores the default minimum value of the MSS for a TCP6 connection.

The default minimum MSS value for a TCP6 connection is 216 bytes.

NOTE

This function takes effect only for TCP6 packets transmitted over a TCP6 connection established with the local device.

Format

tcp ipv6 min-mss *mss-value*

undo tcp ipv6 min-mss

Parameters

Parameter	Description	Value
mss-value	Specifies the minimum MSS value for a TCP6 connection.	The value ranges from 32 byte to 1500 bytes. By default, the value is 216 bytes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To establish a TCP6 connection, the MSS value is negotiated, which indicates the maximum length of packets that the local device can receive. The TCP6 client on a network may send a request packet for establishing a TCP6 connection carrying a small MSS value. For example, the MSS value is 1. After the TCP6 server receives the request packet carrying the MSS value, the TCP6 connection is established. The TCP6 client then may send large numbers of requests to the server by an application, causing the TCP6 server to generate large numbers of reply packets. This may burden the TCP6 server or network, causing denial of service (DoS)

Copyright © Huawei Technologies Co., Ltd.

attacks. To resolve this problem, run the **tcp ipv6 min-mss** command to set the minimum MSS value for a TCP6 connection. This configuration prevents a server from receiving packets carrying a small MSS value.

Precautions

If the **tcp ipv6 min-mss** command is run more than once in the same view, the latest configuration overrides the previous one.

Configure the parameters under the guidance of the technical personnel.

Example

Set the minimum MSS value for a TCP6 connection to 512 bytes.

```
<Huawei> system-view
[Huawei] tcp ipv6 min-mss 512
```

Related Topics

8.8.74 tcp ipv6 window

8.8.72 tcp ipv6 timer fin-timeout

Function

The **tcp ipv6 timer fin-timeout** command sets the value of the TCP6 FIN-Wait timer.

The **undo tcp ipv6 timer fin-timeout** command restores the default value of the TCP6 FIN-Wait timer.

By default, the value of the TCP6 FIN-Wait timer is 675s.

Format

tcp ipv6 timer fin-timeout *interval*

undo tcp ipv6 timer fin-timeout

Parameters

Parameter	Description	Value
interval	Specifies the value of the TCP6 FIN-Wait timer.	The value is an integer that ranges from 76 to 3600, in seconds. The default value is 675s.

Views

System view

Default Level

2: Configuration level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When a TCP6 connection changes from FIN_WAIT_1 to FIN_WAIT_2, the TCP FIN-Wait timer is started. If the local device does not receive a packet with the FIN flag after the TCP6 FIN-Wait timer expires, the TCP6 connection is closed.

Precautions

If you run the **tcp ipv6 timer fin-timeout** command multiple times, only the latest configuration takes effect.

You are advised to use this command under the supervision of technical support personnel.

Example

Set the value of the TCP6 FIN-Wait timer to 800s.

```
<Huawei> system-view
[Huawei] tcp ipv6 timer fin-timeout 800
```

Related Topics

8.8.73 tcp ipv6 timer syn-timeout

8.8.74 tcp ipv6 window

8.8.73 tcp ipv6 timer syn-timeout

Function

The **tcp ipv6 timer syn-timeout** command sets the value of the TCP6 SYN-Wait timer.

The **undo tcp ipv6 timer syn-timeout** command restores the default value of the TCP6 SYN-Wait timer.

By default, the value of the TCP6 SYN-Wait timer is 75s.

Format

tcp ipv6 timer syn-timeout *interval*

undo tcp ipv6 timer syn-timeout

Parameters

Parameter	Description	Value
interval	Specifies the value of the TCP6 SYN-Wait timer.	The value is an integer that ranges from 2 to 600, in seconds. The default value is 75s.

Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an SYN packet is sent, the TCP6 SYN-Wait timer is started. If no response packet is received when the TCP6 SYN-Wait timer expires, the TCP6 connection is closed.

Precautions

If you run the **tcp ipv6 timer syn-timeout** command multiple times, only the latest configuration takes effect.

You are advised to use this command under the supervision of technical support personnel.

Example

Set the value of the TCP6 SYN-Wait timer to 100s.

```
<Huawei> system-view
[Huawei] tcp ipv6 timer syn-timeout 100
```

Related Topics

8.8.72 tcp ipv6 timer fin-timeout

8.8.74 tcp ipv6 window

8.8.74 tcp ipv6 window

Function

The **tcp ipv6 window** command sets the size of the packet receive or send buffer of a connection-oriented socket.

The **undo tcp ipv6 window** command restores the default size of the packet receive or send buffer of a connection-oriented socket.

By default, the size of the packet receive or send buffer of a connection-oriented socket is 8K bytes.

Format

tcp ipv6 window *window-size*

undo tcp ipv6 window

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
window-size	Specifies the size of the packet receive or send buffer of a connection-oriented socket.	The value is an integer that ranges from 1 to 32, in K bytes. The default value is 8K bytes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command changes the default size of the packet receive or send buffer. The device uses the default size to establish a TCP6 session.

Precautions

If you run the **tcp ipv6 window** command multiple times, only the latest configuration takes effect.

You are advised to use this command under the supervision of technical support personnel.

Example

Set the size of the packet receive or send buffer of a connection-oriented socket to 4K bytes.

```
<Huawei> system-view
[Huawei] tcp ipv6 window 4
```

Related Topics

8.8.72 tcp ipv6 timer fin-timeout

8.8.73 tcp ipv6 timer syn-timeout

8.9 DHCPv6 Configuration Commands

8.9.1 address prefix

Function

The **address prefix** command configures the network prefix and lifetime in the IPv6 address pool view.

Copyright © Huawei Technologies Co., Ltd.

The **undo address prefix** command deletes the network prefix and lifetime that are configured in the IPv6 address pool view.

By default, no network prefix and lifetime are configured in the IPv6 address pool view.

Format

address prefix [*prefix-name*] *ipv6-prefix/ipv6-prefix-length* [**eui-64**] [**life-time** { *valid-lifetime* | **infinite** } { *preferred-lifetime* | **infinite** }]

address prefix [*prefix-name*] *ipv6-prefix/ipv6-prefix-length* [**eui-64**] [**life-time preferred-lifetime days** *days* [**hours** *hours* [**minutes** *minutes* [**seconds** *seconds*]]] **valid-lifetime days** *days* [**hours** *hours* [**minutes** *minutes* [**seconds** *seconds*]]]]

address prefix [*prefix-name*] *ipv6-prefix/ipv6-prefix-length* [**lock**]

undo address prefix [*prefix-name*] *ipv6-prefix/ipv6-prefix-length* [**lock**]

Parameters

Parameter	Description	Value
prefix-name	Specifies the name of a network prefix.	The value is a string of 1 to 63 case-sensitive characters without spaces.
ipv6-prefix/ipv6-prefix-length	Specifies the network prefix and prefix length.	*ipv6-prefix*: The value has 128 bits. It is represented as eight groups of four hexadecimal digits with the groups being separated by colons, in the format of X:X:X:X:X:X:X:X. *ipv6-prefix-length*: The value is an integer that ranges from 1 to 128.
eui-64	Generates the interface ID based on the user MAC address according to the EUI-64 specifications. This method can be used to allocate addresses only when the client DUID type is LL or LLT.	-
life-time	Specifies the network prefix lifetime.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
valid-lifetime	Specifies the valid lifetime.	The value is an integer that ranges from 60 to 172799999, in seconds. The default value is 172800, that is two days.
preferred-lifetime	Specifies the preferred lifetime. The preferred lifetime cannot exceed the valid lifetime.	The value is an integer that ranges from 60 to 172799999, in seconds. The default value is 86400, that is one day.
infinite	Sets the lifetime to infinite. When the preferred lifetime is set to infinite, the valid lifetime must be set to infinite.	-
preferred-lifetime days *days* [**hours** *hours* [**minutes** *minutes* [**seconds** *seconds*]]]	Specifies the preferred lifetime of the IPv6 prefix. The time must be no less than 1 minute.	• *days*: indicates days. The value is an integer that ranges from 0 to 1999. • *hours*: indicates hours. The value is an integer that ranges from 0 to 23. • *minutes*: indicates minutes. The value is an integer that ranges from 0 to 59. • *seconds*: indicates seconds. The value is an integer that ranges from 0 to 59.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
valid-lifetime days *days* [**hours** *hours* [**minutes** *minutes* [**seconds** *seconds*]]]	Specifies the valid lifetime of the IPv6 prefix. The time must be no less than 1 minute and cannot be less than the preferred lifetime.	• *days*: indicates days. The value is an integer that ranges from 0 to 1999. • *hours*: indicates hours. The value is an integer that ranges from 0 to 23. • *minutes*: indicates minutes. The value is an integer that ranges from 0 to 59. • *seconds*: indicates seconds. The value is an integer that ranges from 0 to 59.
lock	Locks the address prefix.	-

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device functions as a DHCPv6 server, run the **address prefix** command to configure the network prefix in an IPv6 address pool. If IPv6 addresses in an IPv6 address pool have been assigned to DHCPv6 clients, only the value of life-time can be modified.

Precautions

If no DHCPv6 relay agent exists between the DHCPv6 server and client, the length of the network prefix configured to the DHCPv6 server address pool must be longer than or equal to the prefix length of IPv6 addresses of Layer 3 interfaces on the DHCPv6 server.

Idle addresses or prefixes are assigned to DHCPv6 clients from the IPv6 address pool. Reserved addresses, conflicted addresses, and used addresses cannot be assigned to DHCPv6 clients. Reserved addresses include unspecified addresses, multicast addresses, loopback addresses, link-local addresses, NSAP addresses, and anycast addresses (defined in RFC 2526).

You can configure at most three network prefixes.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

An address pool has been created by using the **dhcpv6 pool** command.

Example

Bind the network prefix fc00:1::/64 to the DHCPv6 server address pool pool1 and set the lifetime to infinite.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] address prefix fc00:1::/64 life-time infinite infinite
```

Related Topics

8.9.14 dhcpv6 pool

8.9.2 capwap-ac (IPv6 address pool view)

Function

The **capwap-ac** command configures the AC's IPv6 address in the IPv6 address pool view.

The **undo capwap-ac** command deletes the AC's IPv6 address configured in the IPv6 address pool view.

By default, the AC's IPv6 address is not configured in the IPv6 address pool view.

Format

capwap-ac *ipv6-address*

undo capwap-ac *ipv6-address*

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address for an AC.	The total length is 128 bit, which is divided into eight groups. The 16 bits of each group are represented by four hexadecimal characters. The format is X:X:X:X:X:X:X:X.

Views

IPv6 address pool view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the AC+Fit AP scenario, the AC needs to establish connections with APs. The device functioning as a DHCPv6 server can specify the AC's IPv6 address for an AP. The AP then can connect to the specified AC. The device uses Option52 to carry the AC address.

If the AC and AP are located in the same network segment, the AP sends a broadcast packet to automatically discover the AC. In this case, the configuration of the **capwap-ac** command is optional. If the AC and AP are located in different network segments, you must configure the **capwap-ac** command.

Prerequisites

The IPv6 address pool is created using the **8.9.14 dhcpv6 pool** command.

Precautions

You can run the **capwap-ac** command multiple times to configure the IPv6 addresses of several ACs. The IPv6 addresses of at most eight ACs can be configured in an address pool, and the AC that is configured first takes precedence over the one configured later.

Example

Specify the AC's IPv6 address to fc00:1::1 in pool1 of the DHCPv6 server.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] capwap-ac fc00:1::1
```

Related Topics

8.9.14 dhcpv6 pool

8.9.3 conflict-address expire-time

Function

The **conflict-address expire-time** command sets the aging time for conflicted addresses in the IPv6 address pool.

The **undo conflict-address expire-time** command restores the default aging time of conflicted addresses in the IPv6 address pool.

By default, the aging time of conflicted addresses is 172800s (two days).

Format

conflict-address expire-time *expire-time*

undo conflict-address expire-time

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
expire-time	Specifies the aging time for the conflicted addresses in the address pool.	The value is an integer that ranges from 60 to 4294967295, in seconds.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **conflict-address expire-time** command is used on DHCPv6 servers. If the IPv6 address in the address pool is marked as a conflicted address, it cannot be allocated. To use these conflicted addresses, the administrator needs to mark these addresses as assignable. After the aging time configured using the **conflict-address expire-time** command expires, the conflicted addresses automatically become assignable.

Prerequisites

An address pool has been created by using the **dhcpv6 pool** command.

Example

Set the aging time of conflicted addresses in global address pool global1 to 36000s.

```
<Huawei> system-view
[Huawei] dhcpv6 pool global1
[Huawei-dhcpv6-pool-global1] conflict-address expire-time 36000
```

Related Topics

8.9.14 dhcpv6 pool

8.9.4 dhcpv6 client information-request

Function

The **dhcpv6 client information-request** command enables an interface to obtain configuration parameters (not including IPv6 addresses) using stateless DHCPv6 address autoconfiguration.

Copyright © Huawei Technologies Co., Ltd.

The **undo dhcpv6 client information-request** command disables an interface from obtaining configuration parameters (not including IPv6 addresses) using stateless DHCPv6 address autoconfiguration.

By default, the interface is disabled from obtaining configuration parameters (not including IPv6 addresses) using stateless DHCPv6 address autoconfiguration.

Format

dhcpv6 client information-request

undo dhcpv6 client information-request

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcpv6 client information-request** command is used on the DHCPv6 client. After you run the **dhcpv6 client information-request** on the WAN-side Layer 3 interface or sub-interface of the device that functions as a DHCPv6 client, IPv6 addresses are generated based on the Route Advertisement (RA) packets. The DHCPv6 server provides other configuration parameters such as IP addresses of the DNS, and SNTP servers except for IPv6 addresses and the interval for updating configuration parameters.

Prerequisites

1. IPv6 functions have been enabled globally using the **8.8.20 ipv6** command in the system view.
2. IPv6 functions have been enabled on interfaces using the **8.8.28 ipv6 enable (interface view)** command in the interface view.
3. The IPv6 link-local address has been configured using the **ipv6 address auto link-local** or **ipv6 address** *ipv6-address* **link-local** command in the interface view.

Precautions

The interval for updating configuration parameters is determined by the DHCPv6 server configuration. If the AR functions as a DHCPv6 server, you can run the **8.9.41 information-refresh** command to configure the interval for updating the configuration parameters obtained using stateless DHCPv6 address autoconfiguration. Limit the interval between 600 to 259200 seconds to prevent a long interval from causing the inconsistency in DNS information on the DHCPv6

Copyright © Huawei Technologies Co., Ltd.

client and server and prevent a short interval from causing the client to frequently request the updated configuration parameters from the server. When the interval in the DHCPv6 server configuration is longer than 259200 seconds (3 days), the interval on the DHCPv6 client is 259200 seconds (3 days). When the interval in the DHCPv6 server configuration is shorter than 600 seconds, the interval on the DHCPv6 client is 600 seconds. When the interval in the DHCPv6 server configuration is between 600 and 259200 seconds, the interval on the DHCPv6 client is the same as the interval in the DHCPv6 server configuration.

Example

Configure the DHCPv6 client to obtain configuration parameters using stateless DHCPv6 address autoconfiguration on the interface GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 address auto link-local
[Huawei-GigabitEthernet1/0/0] dhcpv6 client information-request
```

Related Topics

8.9.28 display dhcpv6 client statistics

8.9.50 reset dhcpv6 client statistics

8.9.26 display dhcpv6 client

8.9.5 dhcpv6 client pd

Function

The **dhcpv6 client pd** command configures the DHCPv6 PD client function.

The **undo dhcpv6 client pd** command disables the DHCPv6 PD client function.

By default, the DHCPv6 PD client function is disabled.

Format

dhcpv6 client [**dhcp** [**hint** *ipv6-address*]] **pd** *prefix-name* [**hint** *ipv6-prefix/ipv6-prefix-length*] [**rapid-commit**] [**unicast-option**]

dhcpv6 client dhcp [**hint** *ipv6-address*] **pd** *prefix-name* [**hint** *ipv6-prefix/ipv6-prefix-length*] [**rapid-commit**] [**unicast-option**] **union-mode**

undo dhcpv6 client [**dhcp**] **pd**

Parameters

Parameter	Description	Value
dhcp	Indicates that a client obtains both an IPv6 address and a prefix.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hint *ipv6-address*	Specifies the required IPv6 address to be requested.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
prefix-name	Specifies the name of an IPv6 address prefix name.	The value is a string of 1 to 63 case-sensitive characters without spaces.
hint *ipv6-prefix/ipv6-prefix-length*	Specifies the required IPv6 address prefix and prefix length.	*ipv6-prefix*: The value has 128 bits. It is represented as eight groups of four hexadecimal digits with the groups being separated by colons, in the format of X:X:X:X:X:X:X:X. *ipv6-prefix-length*: The value is an integer that ranges from 1 to 128.
rapid-commit	Indicates that the DHCPv6 PD client requests an IPv6 address prefix using the two-message exchange.	-
unicast-option	Indicates that the DHCPv6 PD client requests an IPv6 address prefix using the unicast mode.	-
union-mode	Indicates that the DHCPv6 PD client obtains both an IPv6 address and a prefix using a packet.	-

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The **dhcpv6 client pd** command is used on the DHCPv6 PD client. After the **dhcpv6 client pd** is executed on the WAN-side Layer 3 interface or sub-interface of the device that functions as a DHCPv6 PD client, the device requests an IPv6 address prefix in the DHCPv6 mode. The requested prefix is bound to the configured prefix name. You can specify the **hint** *ipv6-prefix/ipv6-prefix-length* parameter to set the required IPv6 address prefix and prefix length.

Prerequisites

1. IPv6 functions have been enabled globally using the **8.8.20 ipv6** command in the system view.
2. IPv6 functions have been enabled on interfaces using the **8.8.28 ipv6 enable (interface view)** command in the interface view.
3. The IPv6 link-local address has been configured using the **ipv6 address auto link-local**, or **ipv6 address** *ipv6-address* **link-local** command in the interface view. Or the IPv6 global unicast IPv6 address has been configured using the **ipv6 address** { *ipv6-address prefix-length* | *ipv6-address*|*prefix-length* } command in the interface view.

Configuration Precautions

When configuring the DHCPv6 PD client function, you cannot set *prefix-name* to **a**, **au**, **aut**, or **auto**. These prefix names cannot be applied to interfaces.

Example

Configure the DHCPv6 PD client to obtain IPv6 address prefix using stateless DHCPv6 address autoconfiguration on the interface GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 address auto link-local
[Huawei-GigabitEthernet1/0/0] dhcpv6 client pd huawei
```

8.9.6 dhcpv6 duid

Function

The **dhcpv6 duid** command configures a DUID for the DHCPv6 device.

By default, the device generates a DUID based on the link-layer (LL) address.

Format

dhcpv6 duid { **ll** | **llt** | *duid* }

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ll	Configures the device to generate a DUID based on the link-layer address (MAC address).	-
llt	Configures the device to generate a DUID based on the link-layer address (MAC address) plus time.	-
duid	Specifies the DUID of the device.	The value is a hexadecimal string with an even number (in the range of 8 to 28) of characters. The value contains only combinations of digits 0 to 9, uppercase letters A to F, and lowercase letters a to f.

Views

System view

Default Level

3: Management level

Usage Guidelines

A DUID identifies a DHCPv6 device. Each DHCPv6 server or client has a unique DUID. Servers use DUIDs to identify clients and clients use DUIDs to identify servers. When this command is run, a new DUID is stored in the :/dhcp/dhcp-duid.txt file of the storage device. You can run the **display dhcpv6 duid** command to check the DUID of the device.

Example

Configure the device to generate a DUID based on the link-layer address.

```
<Huawei> system-view
[Huawei] dhcpv6 duid ll
Warning: The DHCP unique identifier should be globally-unique and stable. Are you sure to change it?
[Y/N]y
```

Related Topics

8.9.29 display dhcpv6 duid

Copyright © Huawei Technologies Co., Ltd.

8.9.7 dhcpv6 client renew

Function

The **dhcpv6 client renew** command updates the IPv6 address or prefix applied by a DHCPv6 client.

Format

dhcpv6 client renew

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The **dhcpv6 client renew** command applies to only the DHCP client and updates the IPv6 address or prefix applied by the DHCPv6 client.

Example

Manually update the applied IPv6 address.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 address auto dhcp
[Huawei-GigabitEthernet1/0/0] dhcpv6 client renew
```

Manually update the applied IPv6 prefix.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcpv6 client pd myprefix
[Huawei-GigabitEthernet1/0/0] dhcpv6 client renew
```

8.9.8 renew-time-percent rebind-time-percent

Function

The **renew-time-percent rebind-time-percent** command configures the percentage of the lease renewal time and the percentage of the rebinding time in the preferred lifetime of an IPv6 address pool.

The **undo renew-time-percent rebind-time-percent** command restores the default percentage of the lease renewal time and the default percentage of the rebinding time in the preferred lifetime of an IPv6 address pool.

 Copyright © Huawei Technologies Co., Ltd.

By default, the percentage of the lease renewal time in the preferred lifetime of an IPv6 address pool is 50%, and the percentage of the rebinding time is 80%.

Format

renew-time-percent *renew-time-percent* **rebind-time-percent** *rebind-time-percent*

undo renew-time-percent rebind-time-percent

Parameters

Parameter	Description	Value
renew-time-percent	Specifies the percentage of the lease renewal time in the preferred lifetime of an IPv6 address pool.	The value is an integer that ranges from 10 to 89. The default value is 50.
rebind-time-percent	Specifies the percentage of the rebinding time in the preferred lifetime of an IPv6 address pool. The value of *rebind-time-percent* must be greater than that of *renew-time-percent*, and the difference between the values must be greater than or equal to 10.	The value is an integer that ranges from 20 to 99. The default value is 80.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to change the lease renewal time and rebinding time in an IPv6 address pool.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

When planning the lease renewal time and rebinding time, you can run the **address prefix** and **renew-time-percent rebind-time-percent** commands to configure the preferred lifetime and the percentage of the lease renewal time and the percentage of the rebinding time in the preferred lifetime respectively. If the lease renewal time and rebinding time are too short, the lease and renewal time (T1 and T2) of IPv6 addresses allocated to DHCPv6 clients by the DHCPv6 server are too short. As a result, DHCPv6 clients send lease renewal packets frequently. It is recommended that you set the lease renewal time and rebinding time based on the actual usage scenario.

Example

Configure the percentage of the lease renewal time and the percentage of the rebinding time in the preferred lifetime of the IPv6 address pool **test**.

```
<Huawei> system-view
[Huawei] dhcpv6 pool test
[Huawei-dhcpv6-pool-test] renew-time-percent 55 rebind-time-percent 85
```

8.9.9 dhcpv6 interface-id format

Function

The **dhcpv6 interface-id format** command configures the Interface-ID format in DHCPv6 packets.

The **undo dhcpv6 interface-id format** command restores the default Interface-ID format in DHCPv6 packets.

By default, the Interface-ID format in DHCPv6 packets is **default**.

Format

dhcpv6 interface-id format { **default** | **user-defined** *text* }

undo dhcpv6 interface-id format

Parameters

Parameter	Description	Value
default	Specifies the default Interface-ID format. The default Interface-ID format is %04svlan.%04cvlan.%mac:%portname. The values of the S-VLAN and C-VLAN are integers containing four characters. If the length is fewer than four characters, the value is prefixed with 0s. For example, if the outer VLAN value in the DHCPv6 packets received by the device is 11, the inner VLAN value is 22, the inbound interface is VLANIF100, and the device MAC address is 6afe-870b-0000, the Interface-ID generated during the system parsing process is 0011.0022.6afe870b0000:vlanif100.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
user-defined *text*	Specifies a user-defined format as the Interface-ID format. A user-defined format can be: • Format defined by keywords: The Interface-ID is defined based on the keywords supported by the user-defined format. For example, if the name of the device to which the users are connected and the outer VLAN to which the users belong need to be recorded, the user-defined format can be %sysname %svlan. If the device name is HUAWEI and the S-VLAN is 100, the user location information recorded by the Interface-ID is HUAWEI 100. For description of the keywords supported by the user-defined format, see **Table 8-94**. • Format defined by common character strings: The Interface-ID is directly defined as a character string. For example, if all users on an interface are located in the office building named N8, the Interface-ID can be directly defined as N8. • Mixed format: The Interface-ID is defined by both the keywords and common character strings. For example, the Interface-ID can be defined as %sysname N8.	The value is a string of case-sensitive characters without spaces. The character string contains 1 to 251 characters, excluding the quotation marks.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Interface-ID records user access information such as the inbound interfaces of the DHCPv6 packets sent from the clients to the device. The device functions as a DHCPv6 relay or lightweight DHCPv6 relay agent (LDRA). When receiving the request packets sent from the DHCPv6 clients and forwarding the packets to the DHCPv6 server, the device can insert the Interface-ID to the packets to identify the DHCPv6 client location information. The location information can be used by the DHCPv6 server to assign IPv6 addresses and network parameters. You can run the **dhcpv6 interface-id format** command to configure the format of the Interface-ID inserted into DHCPv6 packets.

 Copyright © Huawei Technologies Co., Ltd.

Table 8-94 Description of the keywords supported by the user-defined format

Keyword	Description
duid	Specifies the client ID, including information such as the client MAC address.
sysname	Specifies the device name of the client.
portname	Specifies the name of the inbound interface that receives the DHCPv6 packets sent from the client to the device.
porttype	Specifies the type of the inbound interface that receives the DHCPv6 packets sent from the client to the device. The interface type is specified when the NAS interface is configured in certain scenarios.
iftype	Specifies the type of the inbound interface that receives the DHCPv6 packets sent from the client to the device. The interface type is usually GE.
mac	Specifies the device MAC address.
slot	Specifies the slot number of the DHCPv6 packet sent from the client to the device.
subslot	Specifies the sub-slot number of the DHCPv6 packet sent from the client to the device.
port	Specifies the port number of the DHCPv6 packet sent from the client to the device.
svlan	Specifies the outer VLAN of the DHCPv6 packet sent by the client.
cvlan	Specifies the inner VLAN of the DHCPv6 packet sent by the client.
length	Specifies the total length of the keywords following the length keyword. The length of the length keyword is excluded.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command.

Precautions

- The user-defined format content must be specified between the double quotation marks (""). For example, to configure the user-defined format content as **mac**, run the **dhcpv6 interface-id format user-defined "%mac"** command.

 Copyright © Huawei Technologies Co., Ltd.

- Separators that cannot be digits must be added between the keywords in the user-defined format. Otherwise, the keywords cannot be parsed.
- The symbol % must be prefixed to the keywords in the user-defined format to differentiate them from common character strings. If a digit exists before the symbol % and keyword, the digit refers to the number of characters in the keyword.
- The self-defined content is encapsulated in ASCII format. In addition to the preceding precautions, note the following rules:
  - The symbol \ is an escape character. The symbols %, \, and [] following the escape character indicate themselves. For example, \\ represents the character \.
  - An ASCII character string can contain Arabic numerals, uppercase letters, lowercase letters, and the following symbols: ! @ # $ % ^ & * ( ) _ + | - = \ [ ] { } ; : ' " / ? . , < > `.
  - By default, the length of each keyword in an ASCII character string is the actual length of the keyword.

Example

Configure a user-defined format as the format of the Interface-ID in DHCPv6 packets and the device MAC address as the encapsulated content.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcpv6 interface-id format user-defined "%mac"
```

8.9.10 dhcpv6 interface-id insert enable

Function

The **dhcpv6 interface-id insert enable** command enables the function of adding the Interface-ID option in DHCPv6 packets.

The **undo dhcpv6 interface-id insert enable** command disables the function of adding the Interface-ID option in DHCPv6 packets.

By default, the function of adding the Interface-ID option in DHCPv6 packets is enabled.

Format

dhcpv6 interface-id insert enable

undo dhcpv6 interface-id insert enable

Parameters

None

Views

Interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Interface-ID option records user access information such as the inbound interface of the DHCPv6 Request packets sent from the clients to the device. The user access information can be used by the DHCPv6 server to assign IPv6 addresses and network parameters. When the device functions as a DHCPv6 relay agent or lightweight DHCPv6 relay agent (LDRA), and the device receives the Request packets sent from the DHCPv6 clients and forwards the packets to the DHCPv6 server, the device adds the Interface-ID option in the packets to identify location information of the DHCPv6 clients by default. If the DHCPv6 server interconnected to the device does not support the Interface-ID option, you can run the **undo dhcpv6 interface-id insert enable** command to configure the device not to add the Interface-ID option in DHCPv6 packets to flexibly control option information obtained by the DHCPv6 server.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command.

Example

Enable the function of adding the Interface-ID option in DHCPv6 packets on the interface Eth2/0/0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcpv6 interface-id insert enable
```

8.9.11 dhcpv6 packet-rate

Function

The **dhcpv6 packet-rate** command enables rate limit of DHCPv6 messages and sets the rate threshold for DHCPv6 messages.

The **undo dhcpv6 packet-rate** command disables rate limit of DHCPv6 messages and deletes the rate threshold for DHCPv6 messages.

By default, rate limit of DHCPv6 messages is disabled.

Format

dhcpv6 packet-rate *packet-rate*

undo dhcpv6 packet-rate

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
packet-rate	Specifies the rate threshold for DHCPv6 messages.	The value is an integer that ranges from 0 to 400, in pps. If the value is 0, rate limit of DHCPv6 messages is disabled.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent clients from sending a large number of messages to attack the device, the device limits the rate of DHCPv6 messages. After the DHCPv6 packet rate limit is enabled and the rate threshold is configured using the **dhcpv6 packet-rate** command, the DHCPv6 packets are discarded when the packet rate exceeds the rate threshold.

Prerequisites

DHCP functions have been enabled globally using the **dhcp enable** command.

Example

Enable rate limit of DHCPv6 messages and set the rate threshold for DHCPv6 messages to 200 pps.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcpv6 packet-rate 200
```

Related Topics

8.3.18 dhcp enable

8.9.12 dhcpv6 packet-rate drop-alarm enable

Function

The **dhcpv6 packet-rate drop-alarm enable** command enables the alarm function for discarding DHCPv6 messages when the rate of DHCPv6 messages exceeds the limit.

Copyright © Huawei Technologies Co., Ltd.

The **undo dhcpv6 packet-rate drop-alarm enable** command disables the alarm function for discarding DHCPv6 messages when the rate of DHCPv6 messages exceeds the limit.

By default, the alarm function for discarding DHCPv6 messages is disabled when the rate of DHCPv6 messages exceeds the limit.

Format

dhcpv6 packet-rate drop-alarm enable

undo dhcpv6 packet-rate drop-alarm enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the alarm function of DHCPv6 messages discarded is enabled using the **dhcpv6 packet-rate drop-alarm enable** command, the device records alarm information when the number of DHCPv6 packets that are discarded exceeds the alarm threshold. The alarm threshold can be set using the **dhcpv6 packet-rate drop-alarm threshold** command.

Prerequisites

1. DHCP functions have been enabled globally using the **dhcp enable** command.
2. The DHCPv6 packet rate limit has been enabled using the **dhcpv6 packet-rate** command.

Example

Enable the alarm function for discarding DHCPv6 messages when the rate of DHCPv6 messages exceeds rate limit.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcpv6 packet-rate 200
[Huawei] dhcpv6 packet-rate drop-alarm enable
```

Related Topics

8.3.18 dhcp enable

 Copyright © Huawei Technologies Co., Ltd.

8.9.13 dhcpv6 packet-rate drop-alarm threshold

Function

The **dhcpv6 packet-rate drop-alarm threshold** command sets the alarm threshold for the number of DHCPv6 messages discarded when the rate of DHCPv6 messages exceeds the rate limit.

The **undo dhcpv6 packet-rate drop-alarm threshold** command restores the default alarm threshold of the number of DHCPv6 messages discarded.

By default, the alarm threshold is 100 packets when the alarm function of DHCPv6 messages discarded is enabled.

Format

dhcpv6 packet-rate drop-alarm threshold *threshold*

undo dhcpv6 packet-rate drop-alarm threshold

Parameters

Parameter	Description	Value
threshold	Specifies the alarm threshold for the number of DHCPv6 messages discarded when the rate of DHCPv6 messages exceeds the rate limit.	The value is an integer that ranges from 1 to 1000.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the alarm function of DHCPv6 messages discarded is enabled using the **dhcpv6 packet-rate drop-alarm enable** command, the device records alarm information when the number of DHCPv6 packets that are discarded exceeds the alarm threshold.

Prerequisites

1. The DHCP function has been enabled globally using the **dhcp enable** command.

Copyright © Huawei Technologies Co., Ltd.

2. The DHCPv6 packet rate limit has been enabled using the **dhcpv6 packet-rate** *packet-rate* command.
3. The alarm function for discarding DHCPv6 messages when the rate of DHCPv6 messages exceeds the limit has been enabled using the **dhcpv6 packet-rate drop-alarm enable** command.

Example

Configure the device to generate an alarm when the number of DHCPv6 messages discarded exceeds 150 packets.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcpv6 packet-rate 200
[Huawei] dhcpv6 packet-rate drop-alarm enable
[Huawei] dhcpv6 packet-rate drop-alarm threshold 150
```

Related Topics

8.3.18 dhcp enable

8.9.11 dhcpv6 packet-rate

8.9.12 dhcpv6 packet-rate drop-alarm enable

8.9.14 dhcpv6 pool

Function

The **dhcpv6 pool** command creates an IPv6/IPv6 PD address pool or displays the IPv6/IPv6 PD address pool view.

The **undo dhcpv6 pool** command deletes the created IPv6/IPv6 PD address pool.

By default, no IPv6/IPv6 PD address pool is created.

Format

dhcpv6 pool *pool-name*

undo dhcpv6 pool *pool-name*

Parameters

Parameter	Description	Value
pool-name	Specifies the name of an IPv6/IPv6 PD address pool.	The value is a string of 1 to 31 case-sensitive characters without spaces. The value contains digits, letters, underscores (_), and dots (.).

Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The **dhcpv6 pool** command is used on DHCPv6/DHCPv6 PD servers. When configuring the DHCPv6/DHCPv6 PD server, run the **dhcpv6 pool** command to create an IPv6/IPv6 PD address pool for the DHCPv6/DHCPv6 PD server to assign IPv6 addresses or prefixes to DHCPv6/DHCPv6 PD clients.

The total number of IPv6 and IPv6 PD address pools that can be configured varies according to the device models:

- AR100, AR120, AR150, AR160, AR200, AR1200, AR2201-48FE, AR2202-48FE or AR2204: 16
- AR2220E, AR2220, AR2240, AR3200 or AR3600: 32

Example

Create an IPv6 address pool **DHCPv6POOL**.

```
<Huawei> system-view
[Huawei] dhcpv6 pool DHCPv6POOL
```

8.9.15 dhcpv6 relay destination

Function

The **dhcpv6 relay destination** command enables the DHCPv6 relay function on interfaces and configures the IPv6 address of the DHCPv6 server or next-hop relay agent.

The **undo dhcpv6 relay destination** command disables the DHCPv6 relay function on an interface.

By default, the DHCPv6 relay function is disabled on an interface.

Format

dhcpv6 relay { **destination** *ipv6-address* | **interface** *interface-type interface-number* }

undo dhcpv6 relay { **destination** *ipv6-address* | **interface** *interface-type interface-number* }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ipv6-address	Specifies the destination address of relay messages, which can be the IPv6 address of the DHCPv6 server or next hop relay agent.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
interface *interface-type interface-number*	Specifies the type and number of the outbound interface of relay messages.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a client applies to a DHCPv6 server on a different network segment for an IPv6 address, you need to deploy a relay agent between the client and the DHCPv6 server. In this manner, the relay agent transmits DHCPv6 messages exchanged between the client and the DHCPv6 server.

You can use the **dhcpv6 relay destination** command to enable the DHCPv6 relay function on an interface.

Prerequisites

The DHCP function has been enabled using the **8.3.18 dhcp enable** command in the system view.

Precautions

The device supports a maximum of eight DHCPv6 servers or next-hop relays.

Example

Enable the DHCPv6 relay function on GE0/0/1 and set the destination address of relay messages to fc00:1::1.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] ipv6
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] ipv6 enable
[Huawei-GigabitEthernet0/0/1] dhcpv6 relay destination fc00:1::1
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

8.3.18 dhcp enable

8.9.33 display dhcpv6 relay

8.9.16 dhcpv6 relay server-select

Function

The **dhcpv6 relay server-select** command configures a DHCPv6 server group for a DHCPv6 relay agent.

The **undo dhcpv6 relay server-select** command deletes a DHCPv6 server group for a DHCPv6 relay agent.

By default, no DHCPv6 server group is configured.

Format

dhcpv6 relay server-select *group-name*

undo dhcpv6 relay server-select

Parameters

Parameter	Description	Value
group-name	Specifies the name of a DHCPv6 server group.	The value is a string of 1 to 32 case-sensitive characters without spaces.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

The **dhcpv6 relay server-select** command is used on DHCPv6 relay agents. When a DHCPv6 client sends DHCPv6 Request packets to a DHCPv6 server through a DHCPv6 relay agent, you can run the **dhcp relay server-select** command to specify a DHCPv6 server group for the DHCPv6 relay agent and configure the IPv6 address of the DHCPv6 server.

Prerequisites

1. A DHCPv6 server group has been created using the **8.9.25 dhcpv6 server group** command.

Copyright © Huawei Technologies Co., Ltd.

2. The IPv6 function has been enabled using the **8.8.28 ipv6 enable (interface view)** command in the interface view.

Precautions

- Each DHCPv6 server group can be bound to multiple interfaces, but each interface can only be bound to one DHCPv6 server group.
- IP addresses of servers in a DHCPv6 server group cannot be on the same network segment with IP addresses of interfaces on the DHCPv6 relay agent.
- If you run the **dhcpv6 relay server-select** command multiple times in the same interface view, only the latest configuration takes effect.

Example

Configure the DHCPv6 server group named group 1 for the DHCPv6 relay agent on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] dhcp enable
[Huawei] dhcpv6 server group group1
[Huawei-dhcpv6-server-group-group1] dhcpv6-server fc00:1::1
[Huawei-dhcpv6-server-group-group1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] dhcpv6 relay server-select group1
```

Related Topics

8.9.25 dhcpv6 server group

8.9.23 dhcpv6-server

8.9.33 display dhcpv6 relay

8.9.17 dhcpv6 relay source-interface

Function

The **dhcpv6 relay source-interface** command configures the IPv6 address of an interface as the source IPv6 address of packets.

The **undo dhcpv6 relay source-interface** command restores the default setting.

By default, the IPv6 address of an interface is not configured as the source IPv6 address of packets.

Format

dhcpv6 relay source-interface *interface-type interface-number*

undo dhcpv6 relay source-interface

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the interface type and number. • *interface-type*: specifies the interface type. Currently, only loopback interfaces are supported. • *interface-number*: specifies the interface number.	-

Views

System view, interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When forwarding packets from a DHCPv6 client, a DHCPv6 relay agent uses the IPv6 address of the packet inbound interface as the source IPv6 address of the packets. Therefore, you need to configure an IPv6 address for each interface on the DHCPv6 relay agent. As a result, the configuration is complex and IPv6 addresses may be wasted. You can run the **dhcpv6 relay source-interface** *interface-type interface-number* command on the DHCPv6 relay agent to specify the IPv6 address of the loopback interface as the source IPv6 address of the DHCPv6 relayed packets, simplifying the configuration and saving IPv6 addresses.

Prerequisites

Before you run this command in the system view, the first four conditions must be met. Before you run this command in the interface view, all the following conditions must be met.

- The device has been enabled to forward IPv6 unicast packets using the **8.8.20 ipv6** command.
- A loopback interface has been created using the **5.20.10 interface loopback** *loopback-number* command.
- An IPv6 address has been configured for the loopback interface using the **8.8.21 ipv6 address** command.
- DHCP has been enabled globally using the **8.3.18 dhcp enable** command.
- In the interface view:

 Copyright © Huawei Technologies Co., Ltd.

- The IPv6 function has been enabled on the interface using the **8.8.28 ipv6 enable (interface view)** command.
- The DHCPv6 relay function has been enabled on the interface using the **dhcpv6 relay** { **destination** *ipv6-address* | **interface** *interface-type interface-number* } or **dhcpv6 relay server-select** *group-name* command.

Precautions

If an IPv6 address is configured for the inbound interface that receives packets from DHCPv6 clients, the IPv6 address is used as the source IPv6 address of packets.

This command takes effect on all interfaces of the device if it is configured in the system view, and takes effect only on an interface if it is configured in the interface view. If this command is configured in both the interface view and system view, the configuration in the interface view takes effect.

Example

In the system view, configure the IPv6 address of a loopback interface as the source IPv6 address of packets.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface loopback 5
[Huawei-LoopBack5] ipv6 enable
[Huawei-LoopBack5] ipv6 address fc01:1::1/128
[Huawei-LoopBack5] quit
[Huawei] dhcp enable
[Huawei] dhcpv6 relay source-interface loopback 5
```

On VLANIF100, configure the IPv6 address of a loopback interface as the source IPv6 address of packets.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface loopback 5
[Huawei-LoopBack5] ipv6 enable
[Huawei-LoopBack5] ipv6 address fc01:1::1/128
[Huawei-LoopBack5] quit
[Huawei] dhcp enable
[Huawei] interface Vlanif 100
[Huawei-Vlanif100] ipv6 enable
[Huawei-Vlanif100] dhcpv6 relay destination fc00:1::1
[Huawei-Vlanif100] dhcpv6 relay source-interface loopback 5
```

Related Topics

8.8.20 ipv6

8.8.21 ipv6 address

8.3.18 dhcp enable

8.8.28 ipv6 enable (interface view)

8.9.15 dhcpv6 relay destination

8.9.18 dhcpv6 relay option79 insert enable

Copyright © Huawei Technologies Co., Ltd.

Function

The **dhcpv6 relay option79 insert enable** command inserts the Option79 field into DHCPv6 messages.

The **undo dhcpv6 relay option79 insert enable** command restores the default setting.

By default, the Option79 field is not inserted into DHCPv6 messages.

Format

dhcpv6 relay option79 insert enable

undo dhcpv6 relay option79 insert enable

Parameters

None

Views

System view, interface view

Default Level

2: Configuration level

Usage Guidelines

Application Scenario

The MAC address is used to identify the DHCPv4 client on the IPv4 network and the DUID is used to identify the DHCPv6 client on the IPv6 network. In an IPv4 and IPv6 dual-stack service deployment scenario, the administrator wants to establish connections between clients' MAC addresses and IPv4 or IPv6 addresses obtained by the clients and perform unified management over dual-stack clients based on the MAC address. However, the MAC address of the DHCPv6 client cannot be identified using the DUID currently.

As defined in RFC, a DHCPv6 relay agent can fill the link address and link type of a client into the Option79 field. When a device functions as a DHCPv6 relay agent, you can run the **dhcpv6 relay option79 insert enable** command to insert the Option79 field into DHCPv6 messages for enabling the DHCPv6 server to obtain the clients' MAC addresses. When this command is run and the DHCPv6 relay agent receives a Request message from a client, it inserts the Option79 field into the Request message and forwards the message to the DHCPv6 server. The DHCPv6 server then obtains the MAC address of the client by parsing the Option79 field.

Prerequisites

- The DHCPv6 function has been enabled in the system view.
- The DHCPv6 relay function has been enabled in the interface view.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

- Only the first-hop DHCPv6 relay agent supports this function.
- This function takes effect for all interfaces if it is configured in the system view, and takes effect for a specified interface if it is configured in the view of the interface. If this command is configured in both the interface view and system view, the configuration in the interface view takes effect.

Example

Insert the Option79 option into DHCPv6 messages in the system view.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] ipv6
[Huawei] dhcpv6 relay option79 insert enable
```

Insert the Option79 field into DHCPv6 messages in the interface view.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] dhcpv6 relay destination fc00:1::1
[Huawei-GigabitEthernet1/0/0] dhcpv6 relay option79 insert enable
```

8.9.19 dhcpv6 remote-id format

Function

The **dhcpv6 remote-id format** command sets the format of the Remote-ID in DHCPv6 messages.

The **undo dhcpv6 remote-id format** command restores the default format of the Remote-ID in DHCPv6 messages.

By default, the default format of the Remote-ID in DHCPv6 messages is used.

Format

dhcpv6 remote-id format { **default** | **user-defined** *text* }

undo dhcpv6 remote-id format

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
default	Indicates to adopt the default format of the remote ID. The default format of the remote ID is %duid %portname:%04svlan.%04cvlan, where the values of the outer VLAN ID and inner VLAN ID are integers and composed of four characters. If the length is shorter than four characters, 0s are prefixed to the value. For example, if the outer VLAN value in the DHCPv6 packets received by the device is 11, the inner VLAN value is 22, the inbound interface is VLANIF100, and the client DUID is 0003000180FB063545B3, the Remote-ID option generated during the system parsing process is 0003000180FB063545B3 vlanif100:0011.0022.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
user-defined *text*	Specifies a user-defined format as the Remote-ID format. A user-defined format can be: • Format defined by keywords: The Remote-ID is defined based on the keywords supported by the user-defined format. For example, if the name of the device to which the users are connected and the outer VLAN to which the users belong need to be recorded, the user-defined format can be %sysname %svlan. If the device name is HUAWEI and the S-VLAN is 100, the user location information recorded by the Remote-ID is HUAWEI 100. For description of the keywords supported by the user-defined format, see **Table 8-95**. • Format defined by common character strings: The Remote-ID is directly defined as a character string. For example, if all users on an interface are located in the office building named N8, the Remote-ID can be directly defined as N8. • Mixed format: The Remote-ID is defined by both the keywords and common character strings. For	The value is a string of 3 to 247 case-sensitive characters with spaces.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
	example, the Remote-ID can be defined as %sysname N8.	

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

The Remote-ID records user access information such as the DUID of the DHCPv6 packets sent from the clients to the device. The device functions as a DHCPv6 relay or lightweight DHCPfv6 relay agent (LDRA). When receiving the request packets sent from the DHCPv6 clients and forwarding the packets to the DHCPv6 server, the device can insert the Remote-ID to the packets to identify the DHCPv6 client location information. The location information can be used by the DHCPv6 server to assign IPv6 addresses and network parameters. You can run the **dhcpv6 remote-id format** command to configure the format of the Remote-ID inserted into DHCPv6 packets.

Table 8-95 Description of the keywords supported by the user-defined format

Keyword	Description
duid	Specifies the client ID, including information such as the client MAC address.
sysname	Specifies the device name of the client.
portname	Specifies the name of the inbound interface that receives the DHCPv6 packets sent from the client to the device.
porttype	Specifies the type of the inbound interface that receives the DHCPv6 packets sent from the client to the device. The interface type is specified when the NAS interface is configured in certain scenarios.
iftype	Specifies the type of the inbound interface that receives the DHCPv6 packets sent from the client to the device. The interface type is usually GE.

 Copyright © Huawei Technologies Co., Ltd.

Keyword	Description
mac	Specifies the device MAC address.
slot	Specifies the slot number of the DHCPv6 packet sent from the client to the device.
subslot	Specifies the sub-slot number of the DHCPv6 packet sent from the client to the device.
port	Specifies the port number of the DHCPv6 packet sent from the client to the device.
svlan	Specifies the outer VLAN of the DHCPv6 packet sent by the client.
cvlan	Specifies the inner VLAN of the DHCPv6 packet sent by the client.
length	Specifies the total length of the keywords following the length keyword. The length of the length keyword is excluded.

Follow-up Procedure

When the device functions as a DHCPv6 relay, you must run the **8.9.20 dhcpv6 remote-id insert enable** command to enable the function of inserting the Remote-ID into DHCPv6 relay packets after running the **dhcpv6 remote-id format** command to configure the Remote-ID format in DHCPv6 packets.

NOTE

When the device functions as an LDRA, the Remote-ID is inserted into DHCPv6 relay packets by default and the function does not need to be enabled.

Precautions

- The user-defined format content must be specified between the double quotation marks (""). For example, to configure the user-defined format content as **mac**, run the **dhcpv6 interface-id format user-defined "%mac"** command.
- Separators that cannot be digits must be added between the keywords in the user-defined format. Otherwise, the keywords cannot be parsed.
- The symbol % must be prefixed to the keywords in the user-defined format to differentiate them from common character strings. If a digit exists before the symbol % and keyword, the digit refers to the number of characters in the keyword.
- The self-defined content is encapsulated in ASCII format. In addition to the preceding precautions, note the following rules:
  - The symbol \ is an escape character. The symbols %, \, and [] following the escape character indicate themselves. For example, \\ represents the character \.

Copyright © Huawei Technologies Co., Ltd.

- An ASCII character string can contain Arabic numerals, uppercase letters, lowercase letters, and the following symbols: ! @ # $ % ^ & * ( ) _ + | - = \ [ ] { } ; : ' " / ? . , < > `.
- By default, the length of each keyword in an ASCII character string is the actual length of the keyword.

Example

Set the customized format for the remote ID carried in DHCPv6 messages and encapsulate the MAC address of the device into the remote ID.

```
<Huawei> system-view
[Huawei] dhcpv6 remote-id format user-defined "%mac"
```

Related Topics

8.9.20 dhcpv6 remote-id insert enable

8.9.20 dhcpv6 remote-id insert enable

Function

Using the **dhcpv6 remote-id insert enable** command, you can enable the function of appending the remote ID to DHCPv6 relay messages.

Using the **undo dhcpv6 remote-id insert enable** command, you can disable the function of appending the remote ID to DHCPv6 relay messages.

By default, the function of appending the remote ID to DHCPv6 relay messages is disabled.

Format

dhcpv6 remote-id insert enable

undo dhcpv6 remote-id insert enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

The remote ID carries information about a client and identifies a client. The DHCPv6 server can make decisions about address allocation, parameter setting,

 Copyright © Huawei Technologies Co., Ltd.

and prefix agent according to the remote ID. The remote ID is defined by the vendor. Usually, the remote ID carries the phone number of the caller in dialing, user name, IP address of the peer in a point-to-point connection, and access interface.

Prerequisite

1. The IPv6 function has been enabled using the **8.8.28 ipv6 enable (interface view)** command in the interface view.
2. An IPv6 address has been assigned to the DHCPv6 server using the **8.9.15 dhcpv6 relay destination** command in the interface view or the a DHCPv6 server group has been specified for the DHCPv6 relay agent using the **8.9.16 dhcpv6 relay server-select** command.

Example

Enable the function of appending the remote ID to DHCPv6 relay messages on GE0/0/1.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] dhcpv6 remote-id insert enable
```

Related Topics

8.3.18 dhcp enable

8.9.19 dhcpv6 remote-id format

8.9.21 dhcpv6 server (system view)

Function

The **dhcpv6 server** command enables the DHCPv6 server or DHCPv6 PD server function in the system view.

The **undo dhcpv6 server** command disables the DHCPv6 server or DHCPv6 PD server function in the system view.

By default, the DHCPv6 server or DHCPv6 PD server function is disabled in the system view.

Format

dhcpv6 server { **allow-hint** | **preference** *preference-value* | **rapid-commit** | **unicast** } *

undo dhcpv6 server { **allow-hint** | **preference** | **rapid-commit** | **unicast** } *

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
allow-hint	Specifies the DHCPv6 server to allocate addresses, prefixes, and prefix lengths based on the DHCPv6 client requests. If the **allow-hint** parameter is specified, the server preferentially allocates addresses, prefixes, and prefix lengths based on the client requests. If the address, prefix, and prefix length requested by a client are not within the address pool or have been allocated to another client, the server ignores the client request and allocates another available address, prefix, and prefix length to the client.	-
preference *preference-value*	Specifies the server priority in the Advertise packet sent by the device. The DHCPv6 client selects the server with the highest priority based on the server priority in the Advertise packet to assign IPv6 addresses or prefixes.	The value is an integer that ranges from 0 to 255. By default, the value is 0. A larger value indicates a higher server priority.
rapid-commit	Indicates that the device supports fast address or prefix assignment, that is, two-message exchange.	-
unicast	Specifies unicast communication between the client and server during the address lease renewal process.	-

Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device functions as a DHCPv6 or DHCPv6 PD server, the DHCPv6 or DHCPv6 PD server function can be enabled in the system view or interface view. If the DHCPv6 or DHCPv6 PD server function is enabled in the interface view, the configuration information only takes effect on the interfaces and only one IPv6 address pool can be specified on an interface.

The DHCPv6 or DHCPv6 PD server and DHCPv6 clients are in different link scopes and a DHCPv6 relay exists. If the DHCPv6 or DHCPv6 PD server function is enabled in the interface view, configuration parameters such as IPv6 addresses or prefixes are assigned only to the clients in one network segment connected to the DHCPv6 relay, because only one IPv6 address pool can be specified on an interface. If configuration parameters such as IPv6 addresses or prefixes need to be assigned to the DHCPv6 clients in multiple network segments through the DHCPv6 relay, enable the DHCPv6 or DHCPv6 PD server function in the system view.

The configuration method of enabling the DHCPv6 or DHCPv6 PD server function in the interface view is affected by the physical interface status. If the interface status is Down, the DHCPv6 or DHCPv6 PD server cannot successfully assign network configuration parameters to clients through the DHCPv6 relay. When the DHCPv6 or DHCPv6 PD server function is enabled in the system view and there are multiple reachable routes between the DHCPv6 relay and DHCPv6 or DHCPv6 PD server, configuration parameters such as IPv6 addresses can be assigned to clients through the DHCPv6 relay as long as one route between the DHCPv6 relay and DHCPv6 or DHCPv6 PD server is reachable. This improves reliability of the configuration information obtained by the clients. In addition, no configuration is required on the interface, which reduces the administrator's maintenance workload.

When functioning as a DHCPv6 or DHCPv6 PD server, the device may be configured with multiple IPv6 address pools. After receiving the DHCPv6 request packets, the DHCPv6 or DHCPv6 PD server chooses the IPv6 address pool based on the following rules:

- When the device functions as the DHCPv6 server:
  - If a relay exists, the server chooses the address pool that belongs to the same link scope with the configured network prefix (using the **8.9.43 link-address** command or **8.9.1 address prefix**) based on the first link-address field that is not 0. The link-address field identifies the link scope of the DHCPv6 clients.
  - If no relay exists, the device that functions as the DHCPv6 server only assigns configuration parameters to clients in DHCPv6 stateless mode. This indicates that the DHCPv6 server only assigns configuration

 Copyright © Huawei Technologies Co., Ltd.

parameters excluding IPv6 addresses and including DNS, NIS, and SNTP servers, and the IPv6 addresses for clients are automatically generated based on the RA packets. To enable the DHCPv6 server to assign network parameters in DHCPv6 stateful mode, enable the DHCPv6 server function in the interface view, using the **8.9.22 dhcpv6 server (interface view)** command.

- When the device functions as the DHCPv6 PD server:
  - If a relay exists, choose the address pool in the same link scope with the configured network prefix (using the **8.9.43 link-address** command) based on the first link-address field that is not 0. The link-address field identifies the link scope of the DHCPv6 clients.
  - If no relay exists, the DHCPv6 PD server function cannot be enabled in the system view and can be enabled in the interface view, using the **8.9.22 dhcpv6 server (interface view)** command.

Prerequisites

1. The DHCP function has been enabled globally using the **dhcp enable** command.
2. The IPv6 function has been enabled globally using the **ipv6** command.

Example

Enable the DHCPv6 server function in the system view, and configure the server priority to 255.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] ipv6
[Huawei] dhcpv6 server preference 255
```

Related Topics

8.3.18 dhcp enable

8.8.20 ipv6

8.9.22 dhcpv6 server (interface view)

Function

The **dhcpv6 server** command enables the DHCPv6 server function on an interface.

The **undo dhcpv6 server** command disables the DHCPv6 server function on an interface.

By default, the DHCPv6 server function on an interface is disabled.

Format

dhcpv6 server *pool-name* [**allow-hint** | **preference** *preference-value* | **rapid-commit** | **unicast**] *

undo dhcpv6 server

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
pool-name	Specifies the name of the DHCPv6 address pool configured on an interface.	The value is a string of 1 to 31 characters without spaces. The value contains digits, letters, underscores (_), and dots (.).
allow-hint	Specifies the DHCPv6 server to allocate addresses, prefixes, and prefix lengths based on the DHCPv6 client requests. If the **allow-hint** parameter is specified, the server preferentially allocates addresses, prefixes, and prefix lengths based on the client requests. If the address, prefix, and prefix length requested by a client are not within the address pool or have been allocated to another client, the server ignores the client request and allocates another available address, prefix, and prefix length to the client.	-
preference *preference-value*	Specifies the priority of the DHCPv6 server carried in the Advertise message sent by the DHCPv6 server. The DHCPv6 client chooses to obtain an IP address or prefix from the DHCPv6 server with the highest priority based on the server priority carried in the Advertise message.	The value is an integer that ranges from 0 to 255. The default value is 0. A larger value indicates a higher priority of the DHCPv6 server.
rapid-commit	Configures the DHCPv6 server to support fast address prefix allocation.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
unicast	Specifies the unicast communication between the DHCPv6 client and DHCPv6 server during IPv6 address lease.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcpv6 server** command is used on DHCP servers. If an IPv6 address pool is referenced by an interface, the interface assigns addresses or address prefixes in the address pool to clients after receiving the DHCPv6 Request messages.

Prerequisites

- DHCP functions have been enabled globally using the **dhcp enable** command.
- IPv6 functions have been enabled globally using the **ipv6** command.
- IPv6 functions have been enabled using the **ipv6 enable** command in the interface view.

Precautions

- The DHCPv6 client function, DHCPv6 relay function, and DHCPv6 server function cannot be enabled on the same interface simultaneously.
- Only one ipv6 address pool can be referenced by an interface.
- If the ipv6 address pool referenced by the interface does not exist, the DHCPv6 server function does not take effect.

Example

Associate DHCPv6 address pool Pool1 with GE 0/0/1 and set the priority of pool1 to 255.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] ipv6
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] ipv6 enable
[Huawei-GigabitEthernet0/0/1] dhcpv6 server pool1 preference 255
```

 Copyright © Huawei Technologies Co., Ltd.

8.9.23 dhcpv6-server

Function

The **dhcpv6-server** command adds a DHCPv6 server or a next-hop relay agent to a DHCPv6 server group.

The **undo dhcpv6-server** command deletes a DHCPv6 server or a next-hop relay agent that is configured in a DHCPv6 server group.

By default, no DHCPv6 server or next-hop relay agent is configured in a DHCPv6 server group.

Format

dhcpv6-server *ipv6-address*

undo dhcpv6-server *ipv6-address*

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of a DHCPv6 server or a next-hop relay agent.	The 128-bit IPv6 address is divided into eight groups. Each group contains four hexadecimal digits. The format is X:X:X:X:X:X:X:X.

Views

DHCPv6 server group view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

The **dhcpv6-server** command is used on DHCPv6 relay agents. To ensure that the DHCPv6 relay agent can send DHCPv6 packets to multiple DHCPv6 servers, you can configure multiple DHCPv6 servers in a DHCPv6 server group. Multiple DHCPv6 servers can allocate IPv6 addresses and other network configuration information to DHCPv6 clients through the DHCPv6 relay agent.

A DHCPv6 client and a DHCPv6 server can have multiple DHCPv6 relay agents connected in between. A device functions as a DHCPv6 relay agent. If the device is connected to a DHCPv6 server, you need to specify the IPv6 address for the DHCPv6 server. If the device is connected to a next-hop relay agent, you need to specify the IPv6 address for the next-hop relay agent and specify the IPv6 address

 Copyright © Huawei Technologies Co., Ltd.

of the remote DHCPv6 server or the next-hop relay agent on the next-hop relay agent.

Prerequisites

A DHCPv6 server group has been created using the **8.9.25 dhcpv6 server group** command.

Precautions

If a DHCPv6 relay agent is connected to multiple DHCPv6 servers or next-hop relay agents, repeat this step. A maximum of 20 DHCPv6 servers or next-hop relay agents can be connected to the device.

Example

Add the DHCPv6 server at fc00:1::1 to the DHCPv6 server group named dhcp-srv1.

```
<Huawei> system-view
[Huawei] dhcpv6 server group dhcp-srv1
[Huawei-dhcpv6-server-group-dhcp-srv1] dhcpv6-server fc00:1::1
```

Related Topics

8.9.25 dhcpv6 server group

8.9.35 display dhcpv6 server group

8.9.16 dhcpv6 relay server-select

8.9.24 dhcpv6 server database

Function

The **dhcpv6 server database** command enables the device to save DHCPv6 data to storage devices.

The **undo dhcpv6 server database** command disables the device from saving DHCPv6 data to storage devices.

By default, the device is disabled from saving DHCPv6 data to storage devices.

Format

dhcpv6 server database *url* [**write-delay** *interval*]

undo dhcpv6 server database *url*

Parameters

Parameter	Description	Value
url	Specifies the path and name of the file that data is saved to.	The value is a string of 1 to 63 case-insensitive characters without spaces.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
write-delay *interval*	Specifies the interval at which DHCPv6 data is saved.	The value is an integer ranging from 300 to 86400, in seconds. The default value is 86400 seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device functions as a DHCPv6 or DHCPv6 PD server, run the **dhcpv6 server database** command to enable the device to save DHCPv6 data to storage devices. This avoids data loss caused by device faults. DHCPv6 data includes the last data recording time, address pool name, client DUID, IAID, address and prefix bound to the client DUID and IAID, conflicted address, and conflict detection time.

The device automatically saves current DHCPv6 data at the specified interval, and previous data files are overwritten. The interval can be set using the **write-delay** *interval* parameter.

Precautions

If the DHCPv6 client requests for lease renewal when the device (functioning as the DHCPv6 server) restarts, the device cannot receive the renewal request and the client fails to renew the lease.

Example

Configure the device to save DHCP data to the path flash:/dhcpv6.tbl and set the interval for saving data to 36000s.

```
<Huawei> system-view
[Huawei] dhcpv6 server database flash:/dhcpv6.tbl write-delay 36000
```

8.9.25 dhcpv6 server group

Function

The **dhcpv6 server group** command creates a DHCPv6 server group and enters the DHCPv6 server group view, or enters the view of a DHCPv6 server group that has been created.

The **undo dhcpv6 server group** command deletes a created DHCPv6 server group.

Copyright © Huawei Technologies Co., Ltd.

By default, no DHCPv6 server group is created.

Format

dhcpv6 server group *group-name*

undo dhcpv6 server group *group-name*

Parameters

Parameter	Description	Value
group-name	Specifies the name of a DHCPv6 server group.	The value is a string of 1 to 32 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

The **dhcpv6 server group** command is used on DHCPv6 relay agents. Generally, a DHCPv6 relay agent serves multiple DHCPv6 servers. You can run the **dhcpv6 server group** command to create a DHCPv6 server group to manage all the DHCPv6 servers that share the DHCPv6 relay agent. The DHCPv6 server group allocates IPv6 addresses and other network configuration information to users connected to the DHCPv6 relay agent.

Follow-up Procedure

- After a DHCPv6 server group is configured, run the **dhcpv6-server** command to add DHCPv6 servers to the DHCPv6 server group.
- When configuring IP address for DHCPv6 servers, run the **dhcpv6 relay server-select** command on an interface to select the DHCPv6 server group of the DHCPv6 relay agent.

Precautions

A maximum of 32 DHCPv6 server groups can be configured on the device. A maximum of 20 DHCPv6 servers can be added to a DHCPv6 server group.

Example

Create a DHCPv6 server group named DHCPv6-srv1.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] dhcpv6 server group DHCPv6-srv1
[Huawei-dhcpv6-server-group-DHCPv6-srv1]
```

Related Topics

8.9.23 dhcpv6-server

8.9.35 display dhcpv6 server group

8.9.16 dhcpv6 relay server-select

8.9.26 display dhcpv6 client

Function

The **display dhcpv6 client** command displays DHCPv6 client information.

Format

display dhcpv6 client [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about the DHCPv6 client with the specified interface type and number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display dhcpv6 client** command on the DHCPv6 client to check the address that is applied.

Example

Display the DHCPv6 client information.

```
<Huawei> display dhcpv6 client
Vlanif10 is in stateful DHCPv6 client and DHCPv6-PD client
mode.
Stateful DHCPv6 client is in BOUND state.
Preferred server DUID   : 00030001000098764433
  Reachable via address : FE80::200:98FF:FE76:4433
```


Copyright © Huawei Technologies Co., Ltd.

```
IA NA IA ID 0x000001D1 T1 30 T2 48
  Obtained     : 2018-04-18 15:08:49
  Renews       : 2018-04-18 15:09:19
  Rebinds      : 2018-04-18 15:09:37
  Address      : FC00:3::2
    Lifetime valid 120 seconds, preferred 60 seconds
    Expires at 2018-04-18 15:10:49(99 seconds left)
DNS server     : FC00:4::1
SNTP server    : FC00:9::1
               : FC00:9::2

DHCPv6-PD client is in BOUND state.
Preferred server DUID   : 00030001000098765566
  Reachable via address : FE80::200:98FF:FE76:5566
IA PD IA ID 0x000001D1 T1 40 T2 64
  Prefix name  : test
  Obtained     : 2018-04-18 15:08:37
  Renews       : 2018-04-18 15:09:17
  Rebinds      : 2018-04-18 15:09:41
  Prefix       : 194:2::/48
    Lifetime valid 150 seconds, preferred 80 seconds
    Expires at 2018-04-18 15:11:07(117 seconds left)
DNS server     : FC00:4::1
```

Table 8-96 Description of the display dhcpv6 client command output

Item	Description
Vlanif10 is in stateful DHCPv6 client and DHCPv6-PD client mode.	The VLANIF10 interface is in stateful DHCPv6 client and DHCPv6-PD client mode.
Stateful DHCPv6 client is in BOUND state.	The DHCPv6 client is in BOUND state.
Preferred server DUID	DUID of a DHCPv6 server.
Reachable via address	Source IPv6 address from which a DHCPv6 client receives packets.
Prefix name	IPv6 Prefix name that the DHCPv6 client obtains.
Obtained	Time at which the DHCPv6 client obtains an IPv6 address.
Renews	Time (T1) at which the DHCPv6 client updates the lease extension time.
Rebinds	Time (T2) at which the DHCPv6 client rebinds the lease extension time.
Address	IPv6 address that the DHCPv6 client obtains.
Prefix	IPv6 Prefix that the DHCPv6 client obtains.
Lifetime valid 120 seconds, preferred 60 seconds	The valid lifetime is 120 seconds and preferred lifetime is 60 seconds.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Expires at 2018-04-18 15:10:49(99 seconds left)	The address used by the DHCPv6 client will expire at 2018-04-18 15:10:49, and there are 99 seconds left.
DNS server	IPv6 address of the DNS server that the DHCPv6 client obtains.
SNTP server	IPv6 address of the SNTP server that the DHCPv6 client obtains.

Related Topics

8.9.4 dhcpv6 client information-request

8.9.28 display dhcpv6 client statistics

8.9.50 reset dhcpv6 client statistics

8.9.27 display dhcpv6 client prefix

Function

The **display dhcpv6 client prefix** command displays the IPv6 address prefix obtained by the device.

Format

display dhcpv6 client prefix [**name** *prefix-name*]

Parameters

Parameter	Description	Value
name *prefix-name*	Specifies the IPv6 address prefix name.	The value must be an existing IPv6 address prefix name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **display dhcpv6 client prefix** command to view IPv6 address prefixes on the device that functions as the DHCPv6 client.

Copyright © Huawei Technologies Co., Ltd.

Example

Display information about IPv6 prefix named **aaa** obtained by the device.

```
<Huawei> display dhcpv6 client prefix name aaa
Prefix name       : aaa
  Prefix          : FC00:3::/64
    Life time(sec): valid 172800 preferred 86400
```

Table 8-97 Description of the **display dhcpv6 client prefix** command output

Item	Description
Prefix name	IPv6 address prefix name.
Prefix	IPv6 address prefix.
Life time(sec)	• valid: Period during which an IPv6 address prefix is valid. • preferred: Period during which an IPv6 address prefix is valid since its lease is renewed.

Related Topics

8.9.5 dhcpv6 client pd

8.9.28 display dhcpv6 client statistics

Function

The **display dhcpv6 client statistics** command displays DHCPv6 message statistics on the DHCPv6 client.

Format

display dhcpv6 client statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays DHCPv6 message statistics on a specified interface.	-

Views

All views

Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

When the device functions as a DHCPv6 client, run the **display dhcpv6 client statistics** command to view DHCPv6 message statistics on the DHCPv6 client.

Example

Display DHCPv6 message statistics on the DHCPv6 client.

```
<Huawei> display dhcpv6 client statistics
 Message statistics of interface GigabitEthernet0/0/2:
  Message                 Received
  Advertise               1
  Reply                   1
  Reconfigure             0
  Invalid                 0

  Message                 Sent
  Solicit                 1
  Request                 1
  Confirm                 0
  Renew                   0
  Rebind                  0
  Release                 0
  Decline                 0
  Information-request     0
```

Table 8-98 Description of the display dhcpv6 client statistics command output

Item	Description
Message	Message type.
Received	Number of received messages.
Advertise	Number of Advertise messages received by the DHCPv6 client.
Reply	Number of Reply messages received by the DHCPv6 client.
Reconfigure	Number of Reconfigure messages received by the DHCPv6 client.
Invalid	Number of unknown-type messages received by the DHCPv6 client.
Sent	Number of sent messages.
Solicit	Number of Solicit messages sent by the DHCPv6 client.
Request	Number of Request messages sent by the DHCPv6 client.
Confirm	Number of Confirm messages sent by the DHCPv6 client.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Renew	Number of Renew messages sent by the DHCPv6 client.
Rebind	Number of Rebind messages sent by the DHCPv6 client.
Release	Number of Release messages sent by the DHCPv6 client.
Decline	Number of Decline messages sent by the DHCPv6 client.
Information-request	Number of Information-request messages sent by the DHCPv6 client.

Related Topics

8.9.50 reset dhcpv6 client statistics

8.9.29 display dhcpv6 duid

Function

The **display dhcpv6 duid** command displays the DHCP unique identifier of a DHCPv6 device.

Format

display dhcpv6 duid

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

A DUID identifies a DHCPv6 device. Each DHCPv6 server or client has a DUID. The **display dhcpv6 duid** command displays the DUID of a device.

Example

Display the DUID of a DHCPv6 device.

Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display dhcpv6 duid
The device's DHCPv6 unique identifier: 0001000117C667C280FB063545B3
```

Related Topics

8.9.6 dhcpv6 duid

8.9.30 display dhcpv6 relay configuration

Function

The **display dhcpv6 relay configuration** command displays configuration information about a DHCPv6 relay agent.

Format

display dhcpv6 relay configuration [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays configuration information about the DHCPv6 relay agent with the specified interface type and number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command on a DHCPv6 relay agent to check configuration information about a DHCPv6 relay agent including the source interface information and whether the Option79 field is inserted into DHCP messages.

Example

Display configuration information about a DHCPv6 relay agent.

```
<Huawei> display dhcpv6 relay configuration
DHCPv6 relay running information: global
Source interface:       -
Option79 insert:        enable
DHCPv6 relay running information: Vlanif10
Source interface:       -
Option79 insert:        enable
```


Copyright © Huawei Technologies Co., Ltd.

Table 8-99 Description of the **display dhcpv6 relay configuration** command output

Item	Description
DHCPv6 relay running information	Configuration information about a DHCPv6 relay agent, including configuration information in the global view and interface view.
Source interface	Specifies the interface IPv6 address as the source IPv6 address for sending messages. To configure this item, run the **8.9.17 dhcpv6 relay source-interface** command.
Option79 insert	Whether to insert the Option79 field into DHCPv6 messages. The value can be: • enable: The Option79 field is inserted into DHCPv6 messages. • disable: The Option79 field is not inserted into DHCPv6 messages. To configure this item, run the **8.9.18 dhcpv6 relay option79 insert enable** command.

8.9.31 display dhcpv6 relay statistics

Function

Using the **display dhcpv6 relay statistics** command, you can view the statistics about DHCPv6 messages passing through the DHCPv6 relay agent.

Format

display dhcpv6 relay statistics [**interface** *interface-type interface-number*]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. If no interface is specified, the statistics about all the DHCPv6 messages are displayed. If the interface is specified, the statistics about DHCPv6 messages on the specified interface are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If a device is enabled with the DHCPv6 relay function, the system takes the statistics about DHCPv6 messages passing through the DHCP relay agent. After this command is run, you can view the statistics about DHCPv6 messages passing through the DHCP relay agent.

Example

Display the statistics about DHCPv6 messages on VLANIF 10.

```
<Huawei> display dhcpv6 relay statistics interface vlanif 10
 Interface Vlanif10 :
 MessageType             Receive         Send            Error
 Solicit                 0               0               0
 Advertise               0               0               0
 Request                 0               0               0
 Confirm                 0               0               0
 Renew                   0               0               0
 Rebind                  0               0               0
 Reply                   0               0               0
 Release                 0               0               0
 Decline                 0               0               0
 Reconfigure             0               0               0
 Information-request     0               0               0
 Relay-forward           0               0               0
 Relay-reply             0               0               0
 UnknownType             0               0               0
```

 Copyright © Huawei Technologies Co., Ltd.

Table 8-100 Description of the display dhcpv6 relay statistics command output

Item	Description
Interface	Interface enabled with related DHCPv6 functions.
MessageType	Type of DHCPv6 messages.
Receive	Number of received DHCPv6 messages.
Send	Number of sent DHCPv6 messages.
Error	Number of DHCPv6 messages that fail to be parsed.

Related Topics

8.9.15 dhcpv6 relay destination

8.9.32 display dhcpv6 pool

Function

The **display dhcpv6 pool** command displays the IPv6 address pool configurations.

Format

display dhcpv6 pool [*pool-name* [**allocated** { **address** | **prefix** } | **binding** [*duid*] | **conflict address** | *ipv6-address* | *ipv6-prefix/prefix-length*]]

Parameters

Parameter	Description	Value
pool *pool-name*	Specifies the IPv6 address pool name.	The value is a string of 1 to 31 characters without spaces. The value contains digits, letters, underscores (_), and dots (.).
allocated { **address** | **prefix** }	Specifies IPv6 addresses or IPv6 address prefixes that have been assigned.	-
binding [*duid*]	Specifies addresses that are bound to DUIDs.	The value is a string of 2 to 256 characters in hexadecimal notation. The length of the string is an even.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
conflict address	Specifies the conflicted IPv6 addresses in the IPv6 address pool.	-
ipv6-address	Specifies IPv6 addresses in the IPv6 address pool.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
ipv6-prefix/prefix-length	Specifies IPv6 prefixes in the IPv6 address pool.	The value is a 32-digit hexadecimal number, in the format X:X::X:X/M. The IPv6 address prefix length ranges from 1 to 128.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display dhcpv6 pool** command is used on DHCPv6 servers. The **display dhcpv6 pool** command displays information about IPv6 address pool configurations and dynamic address allocation.

Example

Display information about the IPv6 address pool **pool1**.

```
<Huawei> display dhcpv6 pool pool1
DHCPv6 pool: pool1
  Address prefix: FC00:1::/64
    Lifetime valid 4294967295 seconds, preferred 4294967295 seconds
    0 in use, 0 conflicts
  Prefix delegation: FC00:3::/60 64
    Lifetime valid 172800 seconds, preferred 86400 seconds
    0 in use
  Information refresh time: 10000
  DNS server address: FC00:4::1
  SIP server address: FC00:3::1
  NIS server address: FC00:1::2
  NISP server address: FC00:1::2
  SNTP server address: FC00:1::1
  Domain name: huawei.com
  SIP server domain name: sip.com
  NIS server domain name: nis.com
  NISP server domain name: nisp.com
  Vendor-specific option:
    Enterprise ID: 2011
      Suboption 10 address FC00:1::5
```

 Copyright © Huawei Technologies Co., Ltd.

```
conflict-address expire-time: 61
renew-time-percent : 55
rebind-time-percent : 85
Active normal clients: 0
Active pd clients: 0
```

Table 8-101 Description of the **display dhcpv6 pool** command output

Item	Description
DHCPv6 pool	Name of the IPv6 address pool.
Address prefix	Prefix bound to the IPv6 address pool. You can set the prefix using the **8.9.1 address prefix** command.
Prefix delegation	Agent prefix bound to the IPv6 address pool. You can set the agent prefix using the **8.9.49 prefix-delegation** command.
Information refresh time	Time for updating configuration parameters assigned to clients through stateless DHCPv6 address autoconfiguration. You can set the time using the **8.9.41 information-refresh** command.
DNS server address	DNS server address configured for the IPv6 address pool. You can configure the DNS server address using the **8.9.39 dns-server (IPv6 address pool view)** command.
SIP server address	SIP server address configured for the IPv6 address pool. You can configure the SIP server address using the **8.9.56 sip-server (IPv6 address pool view)** command.
NIS server address	NIS server address configured for the IPv6 address pool. You can configure the NIS server address using the **8.9.48 nis-server** command.
NISP server address	NISP server address configured for the IPv6 address pool. You can configure the NISP server address using the **8.9.47 nisp-server** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
SNTP server address	SNTP server address configured for the IPv6 address pool. You can configure the SNTP server address using the **8.9.57 sntp-server** command.
Domain name	Domain name suffix allocated by the DHCPv6 server to the client. You can configure the domain name suffix using the **8.9.38 dns-domain-name** command.
SIP server domain name	SIP domain name suffix allocated by the DHCPv6 server to the client. You can configure the SIP domain name suffix using the **8.9.55 sip-domain-name** command.
NIS server domain name	NIS domain name suffix allocated by the DHCPv6 server to the client. You can configure the NIS domain name suffix using the **8.9.45 nis-domain-name** command.
NISP server domain name	NISP domain name suffix allocated by the DHCPv6 server to the client. You can configure the NISP domain name suffix using the **8.9.46 nisp-domain-name** command.
Vendor-specific option	Vendor-defined options. You can configure the vendor-defined options using the **8.9.61 vendor-specific** and **8.9.60 suboption** commands.
conflict-address expire-time	Aging time of conflicted addresses. You can set the aging time using the **8.9.3 conflict-address expire-time** command.
renew-time-percent	The percentage of the lease renewal time in the preferred lifetime. You can set the percentage of the lease renewal time in the preferred lifetime using the **8.9.8 renew-time-percent rebind-time-percent** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
rebind-time-percent	The percentage of the lease rebinding time in the preferred lifetime. You can set the percentage of the lease rebinding time in the preferred lifetime using the **8.9.8 renew-time-percent rebind-time-percent** command.
Active normal clients	Number of DHCP clients.
Active pd clients	Number of DHCPv6 PD clients.

8.9.33 display dhcpv6 relay

Function

The **display dhcpv6 relay** command displays the configuration of the interface enabled with the DHCPv6 relay function.

Format

display dhcpv6 relay [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the configuration of the specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

If no interface is specified, the configuration of all the interfaces enabled with the DHCPv6 relay function is displayed.

Example

Display the configurations of all interfaces enabled with the DHCPv6 relay function.

```
<Huawei> display dhcpv6 relay
Interface              Mode          Destination
------------------------------------------------------------------------------
GigabitEthernet1/0/1   Relay         FC00:4::3
Vlanif10               Relay         FC00:1::1:1
Vlanif10               Relay         FC00:1::1:2
------------------------------------------------------------------------------
 Print count : 2                  Total count : 2
```

Table 8-102 Description of the **display dhcpv6 relay** command output

Item	Description
Interface	Interface enabled with DHCPv6 relay functions.
Mode	DHCPv6 function mode.
Destination	Destination address of DHCPv6 relay messages. Address pointing to the DHCPv6 server, address of the next-hop DHCPv6 relay, or DHCPv6 server group. To configure the address, run the **8.9.15 dhcpv6 relay destination** or **8.9.16 dhcpv6 relay server-select** command.
Print count	The number of interfaces enabled with DHCPv6 relay functions that are displayed.
Total count	The total number of interfaces enabled with DHCPv6 relay functions.

8.9.34 display dhcpv6 server

Function

The **display dhcpv6 server** command displays information about the DHCPv6 server function.

Format

display dhcpv6 server [**database** | [**statistics**] [**interface** *interface-type interface-number*]]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
database	Displays database configurations.	-
statistics	Displays message statistics on the DHCPv6 server.	-
interface *interface-type interface-number*	Displays information about the DHCP server with a specified interface type and number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display dhcpv6 server** command is used on DHCPv6 servers. The **display dhcpv6 server** command displays information about the DHCPv6 server function.

Example

Display information about the DHCPv6 server function.

```
<Huawei> display dhcpv6 server
 Interface                       DHCPv6 pool
 Vlanif10                        pool1
```

Table 8-103 Description of the **display dhcpv6 server** command output

Item	Description
Interface	Interface enabled with the DHCPv6 server function.
DHCPv6 pool	Name of the IPv6 pool that is configured on the interface. You can configure the IPv6 pool name using the **dhcpv6 server** command.

Related Topics

8.9.14 dhcpv6 pool

Copyright © Huawei Technologies Co., Ltd.

8.9.35 display dhcpv6 server group

Function

The **display dhcpv6 server group** command displays the configuration of a DHCPv6 server group.

Format

display dhcpv6 server group [*group-name*]

Parameters

Parameter	Description	Value
group-name	Displays the configuration of a specified DHCPv6 server group. If this parameter is not specified, the configuration of all DHCPv6 server groups is displayed.	The value is a string of 1 to 32 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Use Scenario

The **display dhcpv6 server group** command is used on DHCPv6 relay agents. You can run the **display dhcpv6 server group** command to view the configuration of DHCPv6 server groups created on a DHCPv6 relay agent.

Prerequisites

DHCPv6 server groups have been configured on the DHCPv6 relay agent using the **dhcpv6 server group** command.

Example

View the configuration of the DHCPv6 server group named group1 on the DHCPv6 relay agent.

Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display dhcpv6 server group group1
 DHCPv6 Group-name   : group1
   (0)   server-ip   : FC00:1::1
```

View the configuration of all the DHCPv6 server groups on the DHCPv6 relay agent.

```
<Huawei> display dhcpv6 server group
dhcpv6 server group
------------------------------------------------------------------------------
 DHCPv6 Group-name   : g1
   (0)   server-ip   : FC00:2::1
   (1)   server-ip   : FC00:2::2
   (2)   server-ip   : FC00:2::3
   (3)   server-ip   : FC00:2::4
   (4)   server-ip   : FC00:2::5
   (5)   server-ip   : FC00:4::1
 DHCPv6 Group-name   : g2
   (0)   server-ip   : FC00:3::111
   (1)   server-ip   : FC00:3::122
   (2)   server-ip   : FC00:3::123
   (3)   server-ip   : FC00:3::124
   (4)   server-ip   : FC00:3::125
   (5)   server-ip   : FC00:3::126
   (6)   server-ip   : FC00:3::127
 DHCPv6 Group-name   : g3
   (0)   server-ip   : FC00:3::1
   (1)   server-ip   : FC00:3::2
   (2)   server-ip   : FC00:3::3
   (3)   server-ip   : FC00:3::4
   (4)   server-ip   : FC00:3::5
   (5)   server-ip   : FC00:3::6
   (6)   server-ip   : FC00:3::7
------------------------------------------------------------------------------
 Total count : 3
```

Table 8-104 Description of the display dhcpv6 server group command output

Item	Description
DHCPv6 Group-name	Name of a DHCPv6 server group. To set this parameter, run the **8.9.25 dhcpv6 server group** command.
server-ip	IPv6 address of a DHCPv6 server in a DHCPv6 server group. To set this parameter, run the **8.9.23 dhcpv6-server** command.

Related Topics

8.9.25 dhcpv6 server group

8.3.59 dhcp-server

8.9.36 display dhcpv6 statistics

Function

The **display dhcpv6 statistics** command displays DHCPv6 packet statistics.

Copyright © Huawei Technologies Co., Ltd.

Format

display dhcpv6 statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The device may become faulty when running the DHCPv6 service. Some fault location methods are required for administrators or device maintenance personnel to locate faults quickly. The most convenient and effective method is to provide statistics about packets and packet loss reasons. Run the **display dhcpv6 statistics** command to view DHCPv6 packet statistics.

Example

View DHCPv6 packet statistics.

```
<Huawei> display dhcpv6 statistics
Input: total 10 packets, discarded 0 packets
  Solicit              :        10,  Advertise            :         0
  Request              :         0,  Confirm              :         0
  Renew                :         0,  Rebind               :         0
  Reply                :         0,  Release              :         0
  Decline              :         0,  Reconfigure          :         0
  Information-request  :         0,  Relay-forward        :         0
  Relay-reply          :         0,  Leasequery           :         0
  Leasequery-reply     :         0,

  Max-user limit       :       831,  Add bindtable failed :       100
Output: total 0 packets, discarded 0 packets
```

Table 8-105 Description of the display dhcpv6 statistics command output

Item	Description
Input: total x packets, discarded y packets	Statistics about DHCPv6 packets received by the device. The number of received DHCPv6 packets is x and the number of discarded DHCPv6 packets is y.
Solicit	Number of SOLICIT packets received by the device.
Advertise	Number of ADVERTISE packets received by the device.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Request	Number of REQUEST packets received by the device.
Confirm	Number of CONFIRM packets received by the device.
Renew	Number of RENEW packets received by the device.
Rebind	Number of REBIND packets received by the device.
Reply	Number of REPLY packets received by the device.
Release	Number of RELEASE packets received by the device.
Decline	Number of DECLINE packets received by the device.
Reconfigure	Number of RECONFIGURE packets received by the device.
Information-request	Number of INFORMATION-REQUEST packets received by the device.
Relay-forward	Number of RELAY-FORW packets received by the device.
Relay-reply	Number of RELAY-REPL packets received by the device.
Leasequery	Number of LEASEQUERY packets received by the device.
Leasequery-reply	Number of LEASEQUERY-REPLY packets received by the device.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Max-user limit or Add bindtable failed	Information displayed if the DHCPv6 service is abnormal. The displayed information includes: • Max-user limit: Total number of DHCP packets discarded because the maximum number of users is exceeded. • Add bindtable failed: Total number of DHCP packets discarded because dynamic binding entries fail to be added. • High cpu occupancy: Total number of DHCP packets discarded because the CPU usage is excessively high. • Port blocked: Total number of DHCP packets discarded because the inbound interface is blocked. • Rx buffers full: Total number of DHCP packets discarded because the remaining queue length is shorter than the reserved threshold. • L2fdb lookup failed: Total number of DHCP packets discarded because entries fail to be queried. • Bad vlan id: Total number of DHCP packets discarded because the VLAN ID is incorrect. • Memory exhausted: Total number of DHCP packets discarded because the memory is exhausted. • L3if protocol down: Total number of DHCP packets discarded because the Layer 3 protocol of the source interface goes Down. • Rate limit: Total number of DHCP packets discarded because rates of the packets exceed the limit. • Bad packet length: Total number of DHCP packets discarded because the packet length is incorrect. • Bad ip header length: Total number of DHCP packets discarded because the IP header length is incorrect. • Bad ip header checksum: Total number of DHCP packets discarded because the checksum of the IP header is incorrect.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• Bad udp checksum: Total number of DHCP packets discarded because the checksum of the UDP header is incorrect. • Hops exceeded: Total number of DHCP packets discarded because the number of next hops is incorrect. • Bad magic cookie: Total number of DHCP packets discarded because the magic-cookie field is incorrect. • Duplicate option: Total number of DHCP packets discarded because the option fields are duplicate. • Bad option length: Total number of DHCP packets discarded because the option field length is incorrect. • End option absent: Total number of DHCP packets discarded because of the incorrect end option. • Dest-port equals source: Total number of DHCP packets discarded because the source interface is also the outbound interface. • Bad chaddr: Total number of DHCP packets discarded because the MAC address of the client is incorrect. • Bad giaddr: Total number of DHCP packets discarded because the relay gateway is incorrect. • Bad request: Total number of DHCP packets discarded because the request packets are incorrect. • Bad reply: Total number of DHCP packets discarded because the response packets are incorrect. • Bad dest udp-port: Total number of DHCP packets discarded because the destination interface is incorrect. • Bad message type: Total number of DHCP packets discarded because of incorrect destination interfaces. • L2fdb lookup failed: Total number of incoming DHCP packets discarded because entries fail to be queried.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• Client transfered: Total number of DHCP packets discarded due to interface flapping. • Bad original interface: Total number of DHCP packets discarded because dynamic binding entries are added. • Bad client-id: Total number of DHCP packets discarded because the client ID is incorrect. • Bad server-id: Total number of DHCP packets discarded because the server ID is incorrect. • Bad dest-ip: Total number of DHCP packets discarded because the destination IP address is incorrect. • Other error: Total number of DHCP packets discarded due to other reasons.
Output: total x packets, discarded y packets	Statistics about DHCPv6 packets sent by the device. The number of sent DHCPv6 packets is x and the number of discarded DHCPv6 packets is y.

8.9.37 display import all

Function

The **display import all** commands displays DNS and SNTP configurations that a DHCPv6 server automatically assigns to a DHCPv6 client.

Format

display import all

Parameters

None

Views

IPv6 address pool view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Run the **8.9.62 import all (IPv6 address pool view)** command on the DHCPv6 server to enable the DHCPv6 server to automatically assign configurations of DNS server and SNTP server to DHCPv6 clients. The **display import all** command displays configurations of DNS server and SNTP server that the DHCPv6 server automatically assigns to DHCPv6 clients.

Example

Display DNS and SNTP configurations that the DHCPv6 server automatically assigns to the DHCPv6 client.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] display import all
-------------------------------------------------------------------------------
Parameter      Update time          Value
-------------------------------------------------------------------------------
dns-server     -                    -
sntp-server    -                    -
-------------------------------------------------------------------------------
```

Table 8-106 Description of **display import all** command output

Item	Description
Parameter	Dynamically assigned information type: • dns-server: DNS server information • sntp-server: SNTP server information To set the dynamically assigned information type, run the **8.9.62 import all (IPv6 address pool view)** command.
Update time	Update time of dynamically assigned information.
Value	Contents of dynamically assigned information.

8.9.38 dns-domain-name

Function

The **dns-domain-name** command configures the DNS domain name suffix assigned by the DHCPv6 server to a DHCPv6 client.

The **undo dns-domain-name** command deletes the assigned domain name suffix.

By default, no DNS domain name suffix is configured for the DHCPv6 client.

Copyright © Huawei Technologies Co., Ltd.

Format

dns-domain-name *dns-domain-name*

undo dns-domain-name *dns-domain-name*

Parameters

Parameter	Description	Value
dns-domain-name	Specifies the DNS domain name suffix assigned to a DHCPv6 client.	The value is a string of 1 to 63 case-insensitive characters without spaces. The value contains letters, digits, underscores (_), and dots (.).

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dns-domain-name** command is used on DHCPv6 servers. The DHCPv6 server specifies a domain name suffix when allocating IPv6 addresses for clients. You can use the **dns-domain-name** command on the DHCPv6 server to specify a domain name for each global address pool. When allocating IPv6 addresses to clients, the DHCPv6 server also sends the domain name suffix to the clients.

Precautions

A maximum of four different DNS domain names can be configured for an IPv6 address pool.

Example

Configure the domain name suffix assigned to the DHCPv6 client as **huawei.com** for the address pool **pool1**.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] dns-domain-name huawei.com
```

Related Topics

8.9.14 dhcpv6 pool

Copyright © Huawei Technologies Co., Ltd.

8.9.39 dns-server (IPv6 address pool view)

Function

The **dns-server** command configures a DNS server address for the DHCPv6 address pool.

The **undo dns-server** command deletes the configured DNS server address.

By default, no DNS server address is configured for the IPv6 address pool.

Format

dns-server *ipv6-address*

undo dns-server *ipv6-address*

Parameters

Parameter	Description	Value
ipv6-address	DNS server IPv6 address configured for the DHCPv6 address pool.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dns-server** command is used on DHCPv6 servers. Before a host accesses the Internet, a DNS server needs to resolve the accessed domain name to an IP address. The DHCPv6 server needs to specify the IPv6 address of the DNS server for the global address pool so that the DHCPv6 client can be connected to the Internet. The DHCPv6 server specifies the IPv6 address of the DNS server when allocating IPv6 addresses to the clients.

Precautions

- To specify multiple DNS servers, run the **dns-server** command to configure multiple DNS server addresses.
- A maximum of two DNS server addresses can be configured for each IPv6 address pool. The first assigned DNS server address is used as a primary address. The priority of the first configured DNS server is higher than that of the other DNS server.

 Copyright © Huawei Technologies Co., Ltd.

Example

Specify a DNS server with the IPv6 address fc00:1::1 for domain name resolution when IP addresses in the address pool **global1** are assigned to clients.

```
<Huawei> system-view
[Huawei] dhcpv6 pool global1
[Huawei-dhcpv6-pool-global1] dns-server fc00:1::1
```

Related Topics

8.9.14 dhcpv6 pool

8.9.40 excluded-address

Function

The **excluded-address** command specifies the range of the IPv6 addresses that cannot be automatically assigned to clients from the IPv6 address pool.

The **undo excluded-address** command deletes the specified range of the IPv6 addresses that cannot be automatically assigned to clients from the address pool.

By default, all IPv6 addresses in the address pool can be automatically assigned to clients.

Format

excluded-address [*prefix-name*] *start-ipv6-address* [**to** *end-ipv6-address*]

undo excluded-address [*prefix-name*] *start-ipv6-address* [**to** *end-ipv6-address*]

Parameters

Parameter	Description	Value
prefix-name	Specifies the name of a network prefix.	The value is a string of 1 to 63 case-sensitive characters without spaces.
start-ipv6-address	Specifies the start IPv6 address that cannot be automatically assigned.	The value has 128 bits. It is represented as eight groups of four hexadecimal digits with the groups being separated by colons, in the format of X:X:X:X:X:X:X:X.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
to *end-ipv6-address*	Specifies the end IPv6 address that cannot be automatically assigned.	The value has 128 bits. It is represented as eight groups of four hexadecimal digits with the groups being separated by colons, in the format of X:X:X:X:X:X:X:X. *end-ipv6-address* and *start-ipv6-address* must be on the same network segment and *end-ipv6-address* must be greater than *start-ipv6-address*. If *end-ipv6-address* is not specified, only the *start-ipv6-address* cannot be automatically assigned.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **excluded-address** command is used on DHCPv6 servers. In an address pool, some IPv6 addresses need to be reserved for other services, and some IPv6 addresses are statically assigned to certain hosts (such as the DNS server and Web server) and cannot be automatically assigned to clients. You can run the **excluded-address** command to specify the range of the IPv6 addresses that cannot be automatically assigned to clients from the IPv6 address pool.

Prerequisites

1. An address pool has been created by using the **dhcpv6 pool** command.
2. Bind an IPv6 address prefix to an address pool by using the **address prefix**

Precautions

- The excluded IPv6 address or IPv6 address segment must be in the local address pool.
- The excluded IPv6 address or IPv6 address segment cannot be automatically assigned to clients from a local address pool.

 Copyright © Huawei Technologies Co., Ltd.

- If you run the **excluded-address** command multiple times, you can specify multiple IPv6 addresses or IPv6 address segments that cannot be automatically assigned to clients.

Example

Specify IPv6 addresses fc00:1::1 to fc00:1::10 not to be automatically allocated from the address pool **global1**.

```
<Huawei> system-view
[Huawei] dhcpv6 pool global1
[Huawei-dhcpv6-pool-global1] address prefix fc00:1::/64
[Huawei-dhcpv6-pool-global1] excluded-address fc00:1::1 to fc00:1::10
```

Related Topics

8.9.14 dhcpv6 pool

8.9.41 information-refresh

Function

The **information-refresh** command configures the time for updating configuration parameters assigned to clients through stateless DHCPv6 address autoconfiguration.

The **undo information-refresh** command restores the default time for updating IPv6 address pool configurations.

By default, the time for updating IPv6 address pool configurations is 86400s (24 hours).

Format

information-refresh *time*

undo information-refresh

Parameters

Parameter	Description	Value
time	Specifies the time for updating configuration parameters assigned to clients through stateless DHCPv6 address autoconfiguration.	The value is an integer that ranges from 600 to 4294967295, in seconds.

Views

IPv6 address pool view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

The **information-refresh** command is used on DHCPv6 servers. When the DHCPv6 server assigns configuration parameters such as the DNS, NIS, and SNTP server addresses to the DHCPv6 clients through stateless autoconfiguration, you can use the **information-refresh** command to configure the time for updating these configuration parameters.

NOTE

If a Huawei device functions as a DHCPv6 client and the time configured using the **information-refresh** command on the DHCPv6 server is larger than three days (259200 seconds), the time for updating DHCPv6 client configuration information is three days. If the time configured using the **information-refresh** command on the DHCPv6 server is less than or equal to three days, the time for updating DHCPv6 client configuration information is the actually configured value.

Example

Set the time for updating configuration parameters assigned to clients to 10000s in the address pool pool1.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] information-refresh 10000
```

Related Topics

8.9.14 dhcpv6 pool

8.9.42 ipv6 address auto dhcp

Function

The **ipv6 address auto dhcp** command enables an interface to obtain IPv6 addresses and other configuration parameters using stateful DHCPv6 address autoconfiguration.

The **undo ipv6 address auto dhcp** command disables an interface from obtaining IPv6 addresses and other configuration parameters using stateful DHCPv6 address autoconfiguration.

By default, the interface is disabled from obtaining IPv6 addresses and other configuration parameters using stateful DHCPv6 address autoconfiguration.

Format

ipv6 address auto dhcp [**hint** *ipv6-address*] [**rapid-commit**] [**unicast-option**]

undo ipv6 address auto dhcp

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
hint *ipv6-address*	Specifies the IPv6 address applied by a DHCPv6 client.	The total length is 128 bit, which is divided into eight groups. The 16 bits of each group are represented by four hexadecimal characters. The format is X:X:X:X:X:X:X:X.
rapid-commit	Specifies that a DHCPv6 client applies for an IPv6 address using two-message exchange.	-
unicast-option	Specifies that a DHCPv6 client applies for an IPv6 address using a unicast option.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you run the **ipv6 address auto dhcp** [**rapid-commit**] command on the WAN-side Layer 3 interface or sub-interface of the device that functions as a DHCPv6 client, the client uses stateful DHCPv6 address autoconfiguration to obtain IPv6 addresses and other configuration parameters, such as addresses of the DNS and SNTP servers, from the DHCPv6 server.

Prerequisites

1. IPv6 functions have been enabled globally using the **8.8.20 ipv6** command in the system view.
2. IPv6 functions have been enabled on interfaces using the **8.8.28 ipv6 enable (interface view)** command in the interface view.
3. The IPv6 link-local address has been configured using the **ipv6 address auto link-local** or **ipv6 address** *ipv6-address* **link-local** command in the interface view.
4. The interface has been configured to automatically learn the IPv6 default route using the **ipv6 address auto global default** command in the interface view.

Precautions

The DHCPv6 server assigns an IPv6 address and other configuration parameters to a DHCPv6 client using two-message exchange only when two-message exchange

 Copyright © Huawei Technologies Co., Ltd.

is configured on both the server and client. If two-message exchange is not configured on the server or client, the server assigns an IPv6 address and other configuration parameters to the client using four-message exchange. Two-message exchange applies to the scenarios with one DHCPv6 server, while four-message exchange applies to the scenarios with multiple DHCPv6 servers.

Example

Configure the interface GE1/0/0 to obtain IPv6 addresses and other configuration parameters from the DHCPv6 server using DHCPv6 stateful address autoconfiguration.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 address auto link-local
[Huawei-GigabitEthernet1/0/0] ipv6 address auto dhcp
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.9.43 link-address

Function

The **link-address** command configures the network prefix in the IPv6 address pool view.

The **undo link-address** command deletes the network prefix configured in the IPv6 address pool view.

By default, no network prefix is configured in the IPv6 address pool view.

Format

link-address *ipv6-prefix/ipv6-prefix-length*

undo link-address *ipv6-prefix/ipv6-prefix-length*

Parameters

Parameter	Description	Value
ipv6-prefix/ipv6-prefix-length	Specifies the network prefix and prefix length.	*ipv6-prefix*: The 128-bit IPv6 address is divided into eight groups. Each group contains four hexadecimal digits. The format is X:X:X:X:X:X:X:X. *ipv6-prefix-length*: The value is an integer that ranges from 16 to 128.

Copyright © Huawei Technologies Co., Ltd.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The DHCPv6 client needs to apply for network configuration information (for example, the IP address of the DNS server) except for the IPv6 address from the DHCPv6 server. If the **8.9.1 address prefix** is not configured in the IPv6 address pool, you can run the **link-address** command to configure the network prefix in the IPv6 address pool view.

When functioning as a DHCPv6 or DHCPv6 PD server, the device may be configured with multiple IPv6 address pools. After receiving the DHCPv6 request packets, the DHCPv6 or DHCPv6 PD server chooses the IPv6 address pool based on the following rules:

- When the device functions as the DHCPv6 server:
  - If a relay exists, the server chooses the address pool that belongs to the same link scope with the configured network prefix (using the **link-address** or **8.9.1 address prefix**command) based on the first link-address field that is not 0. The link-address field identifies the link scope of the DHCPv6 clients.
  - If no relay exists, the device that functions as the DHCPv6 server only assigns configuration parameters to clients in DHCPv6 stateless mode. This indicates that the DHCPv6 server only assigns configuration parameters excluding IPv6 addresses and including DNS, NIS, and SNTP servers, and the IPv6 addresses for clients are automatically generated based on the RA packets. To enable the DHCPv6 server to assign network parameters in DHCPv6 stateful mode, enable the DHCPv6 server function in the interface view, using the **8.9.22 dhcpv6 server (interface view)** command.
- When the device functions as the DHCPv6 PD server:
  - If a relay exists, choose the address pool in the same link scope with the configured network prefix (using the **link-address** command) based on the first link-address field that is not 0. The link-address field identifies the link scope of the DHCPv6 clients.
  - If no relay exists, the DHCPv6 PD server function cannot be enabled in the system view and can be enabled in the interface view, using the **8.9.22 dhcpv6 server (interface view)** command.

Prerequisites

Idle addresses or prefixes are assigned to DHCPv6 clients from the IPv6 address pool. Reserved addresses, conflicted addresses, and used addresses cannot be assigned to DHCPv6 clients. Reserved addresses include unspecified addresses, multicast addresses, loopback addresses, link-local addresses, NSAP addresses, and anycast addresses (defined in RFC 2526).

 Copyright © Huawei Technologies Co., Ltd.

Example

Bind the IPv6 address prefix fc00:1::/64 to the DHCPv6 server address pool named pool1.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] link-address fc00:1::/64
```

8.9.44 lock (IPv6 address pool view)

Function

The **lock** command locks the IPv6 address pool.

The **undo lock** command unlocks the address pool.

By default, the IPv6 address pool is unlocked.

Format

lock

undo lock

Parameters

None

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **lock** command is used on DHCPv6 servers. When a DHCPv6 server needs to be migrated, you simply need to migrate address pools on the DHCPv6 server to another DHCPv6 server on the live network. To retain the addresses that have been assigned to clients from a global address pool, run the **lock** command to lock the global address pool. When new users get online, they apply for IPv6 addresses from a new address pool.

Precautions

After the **lock** command is executed, the IPv6 address pool is locked. The locked IPv6 address pool does not assign addresses or extend address lease but only release addresses.

 Copyright © Huawei Technologies Co., Ltd.

Example

Lock the address pool **global1**.

```
<Huawei> system-view
[Huawei] dhcpv6 pool global1
[Huawei-dhcpv6-pool-global1] lock
```

Related Topics

8.9.14 dhcpv6 pool

8.9.45 nis-domain-name

Function

The **nis-domain-name** command configures the NIS domain name suffix assigned by the DHCPv6 server to a DHCPv6 client.

The **undo nis-domain-name** command deletes the NIS domain name suffix assigned to the DHCPv6 client.

By default, no NIS domain name suffix is configured for the DHCPv6 client.

Format

nis-domain-name *nis-domain-name*

undo nis-domain-name *nis-domain-name*

Parameters

Parameter	Description	Value
nis-domain-name	Specifies the NIS domain name suffix assigned to a DHCPv6 client.	The value is a string of 1 to 63 case-insensitive characters without spaces. The value contains letters, digits, underscores (_), and dots (.).

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Copyright © Huawei Technologies Co., Ltd.

The **nis-domain-name** command is used on DHCPv6 servers. The DHCPv6 server specifies an NIS domain name suffix when allocating IPv6 addresses for clients. You can use the **nis-domain-name** command on the DHCPv6 server to specify a NIS domain name suffix for each global address pool. When allocating IPv6 addresses to clients, the DHCPv6 server also sends the NIS domain name suffix to the clients.

Precautions

A maximum of four different NIS domain names can be configured for an IPv6 address pool.

Example

Configure the NIS domain name assigned to the DHCPv6 client as **nis.com** for the address pool pool1.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] nis-domain-name nis.com
```

Related Topics

8.9.14 dhcpv6 pool

8.9.46 nisp-domain-name

Function

The **nisp-domain-name** command configures the NISP domain name suffix assigned by the DHCPv6 server to a DHCPv6 client.

The **undo nisp-domain-name** command deletes the assigned NISP domain name suffix.

By default, no NISP domain name suffix is configured for the DHCPv6 client.

Format

nisp-domain-name *nisp-domain-name*

undo nisp-domain-name *nisp-domain-name*

Parameters

Parameter	Description	Value
nisp-domain-name	Specifies the NISP domain name suffix assigned to a DHCPv6 client.	The value is a string of 1 to 63 case-insensitive characters without spaces. The value contains letters, digits, underscores (_), and dots (.).

Copyright © Huawei Technologies Co., Ltd.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **nisp-domain-name** command is used on DHCPv6 servers. The DHCPv6 server specifies an NISP domain name suffix when allocating IPv6 addresses for clients. You can use the **nisp-domain-name** command on the DHCPv6 server to specify a NISP domain name for each global address pool. When allocating IPv6 addresses to clients, the DHCPv6 server also sends the domain name suffix to the clients.

Precautions

A maximum of four different NISP domain name suffixes can be configured for an IPv6 address pool.

Example

Configure the NISP domain name assigned to the DHCPv6 client as **nisp.com** for the address pool pool1.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] nisp-domain-name nisp.com
```

Related Topics

8.9.14 dhcpv6 pool

8.9.47 nisp-server

Function

The **nisp-server** command configures the NISP server address assigned to the DHCPv6 client for the IPv6 address pool.

The **undo nisp-server** command deletes the configured NISP server address assigned to the DHCPv6 client from the IPv6 address pool.

By default, no NISP server address is configured for the IPv6 address pool.

Format

nisp-server *ipv6-address*

undo nisp-server *ipv6-address*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ipv6-address	Indicates the NISP server IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **nisp-server** command is used on DHCPv6 servers. The DHCPv6 server needs to specify the IPv6 address of the NISP server for the address pool so that the DHCPv6 client can be connected to the Internet. The DHCPv6 server specifies the IPv6 address of the NISP server when allocating IPv6 addresses to the clients.

Precautions

- A maximum of two NISP server addresses can be configured for each IPv6 address pool. The first assigned address functions as the primary address, and the other address functions as a secondary address.
- When multiple NISP servers are specified, you need to run the **nisp-server** repeatedly to configure multiple addresses.

Example

Specify fc00:1::2 as the IPv6 address of the NISP server when the IPv6 addresses in the address pool global1 are assigned to clients.

```
<Huawei> system-view
[Huawei] dhcpv6 pool global1
[Huawei-dhcpv6-pool-global1] nisp-server fc00:1::2
```

Related Topics

8.9.14 dhcpv6 pool

8.9.48 nis-server

Function

The **nis-server** command configures the NIS server address assigned to the DHCPv6 client for the IPv6 address pool.

Copyright © Huawei Technologies Co., Ltd.

The **undo nis-server** command deletes the configured NIS server address assigned to the DHCPv6 client from the IPv6 address pool.

By default, no NIS server address is configured for the IPv6 address pool.

Format

nis-server *ipv6-address*

undo nis-server *ipv6-address*

Parameters

Parameter	Description	Value
ipv6-address	Indicates the NIS server IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **nis-server** command is used on DHCPv6 servers. The DHCPv6 server needs to specify the IPv6 address of the NIS server for the address pool so that the DHCPv6 client can be connected to the Internet. The DHCPv6 server specifies the IPv6 address of the NIS server when allocating IPv6 addresses to the clients.

Precautions

- A maximum of two NIS server addresses can be configured for each IPv6 address pool. The first assigned address functions as the primary address, and the other address functions as a secondary address.
- When multiple NIS servers are specified, you need to run the **nis-server** repeatedly to configure multiple addresses.

Example

Specify fc00:1::2 as the IPv6 address of the NIS server when IPv6 addresses in the address pool **global1** are assigned to clients.

```
<Huawei> system-view
[Huawei] dhcpv6 pool global1
[Huawei-dhcpv6-pool-global1] nis-server fc00:1::2
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

8.9.14 dhcpv6 pool

8.9.49 prefix-delegation

Function

The **prefix-delegation** command configures an agent prefix in the address pool view.

The **undo prefix-delegation** command deletes the agent prefix in the address pool view.

By default, no IPv6 address agent prefix is configured in the address pool view.

Format

prefix-delegation *ipv6-prefix/ipv6-prefix-length assign-prefix-length* [**life-time** { *valid-lifetime* | **infinite** } { *preferred-lifetime* | **infinite** }]

prefix-delegation *ipv6-prefix/ipv6-prefix-length assign-prefix-length* [**life-time preferred-lifetime days** *days* [**hours** *hours* [**minutes** *minutes* [**seconds** *seconds*]]] **valid-lifetime days** *days* [**hours** *hours* [**minutes** *minutes* [**seconds** *seconds*]]]]

prefix-delegation *ipv6-prefix/ipv6-prefix-length* **lock**

undo prefix-delegation *ipv6-prefix/ipv6-prefix-length* [**lock**]

Parameters

Parameter	Description	Value
ipv6-prefix/ipv6-prefix-length	Specifies the address prefix and the prefix length bound to an IPv6 address pool.	The value is a 32-digit hexadecimal number, in the format X:X::X:X/M. The IPv6 address prefix length ranges from 1 to 128.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
assign-prefix-length	Specifies the default prefix length. **NOTE** If the DHCPv6 server has been configured to allocate prefix lengths based on the DHCPv6 client requests, and the client-requested prefix length is within the range from *ipv6-prefix-length* to *assign-prefix-length*, the server allocates the prefix length based on the client request. If the client-requested prefix length is not within the preceding range or the server is not configured to allocate prefix lengths based on the DHCPv6 client requests, the server allocates the default prefix length. You can run the **dhcpv6 server allow-hint** or **dhcpv6 server** *pool-name* **allow-hint** command to configure the server to allocate prefix lengths based on the DHCPv6 client requests.	The value is an integer that ranges from 1 to 128. The *assign-prefix-length* must be greater than or equal to *ipv6-prefix-length*. The difference between the *assign-prefix-length* and *ipv6-prefix-length* must be less than or equal to 16.
life-time	Specifies the lifetime of the address prefix bound to an IPv6 address pool.	-
valid-lifetime	Specifies the valid lifetime.	The value ranges from 60 to 172799999, in seconds. The default value is 172800, that is two days.
preferred-lifetime	Specifies the preferred lifetime. The preferred lifetime cannot exceed the valid lifetime.	The value ranges from 60 to 172799999, in seconds. The default value is 86400, that is one day.
infinite	Sets the lifetime to infinite. When the preferred lifetime is set to infinite, the valid lifetime must be set to infinite.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
preferred-lifetime days *days* [**hours** *hours* [**minutes** *minutes* [**seconds** *seconds*]]]	Specifies the preferred lifetime of the IPv6 prefix. The time must be no less than 1 minute.	• *days*: indicates days. The value is an integer that ranges from 0 to 1999. • *hours*: indicates hours. The value is an integer that ranges from 0 to 23. • *minutes*: indicates minutes. The value is an integer that ranges from 0 to 59. • *seconds*: indicates seconds. The value is an integer that ranges from 0 to 59.
valid-lifetime days *days* [**hours** *hours* [**minutes** *minutes* [**seconds** *seconds*]]]	Specifies the valid lifetime of the IPv6 prefix. The time must be no less than 1 minute and cannot be less than the preferred lifetime.	• *days*: indicates days. The value is an integer that ranges from 0 to 1999. • *hours*: indicates hours. The value is an integer that ranges from 0 to 23. • *minutes*: indicates minutes. The value is an integer that ranges from 0 to 59. • *seconds*: indicates seconds. The value is an integer that ranges from 0 to 59.
lock	Locks the address prefix.	-

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device functions as a DHCPv6 PD server, run the **prefix-delegation** command to configure an agent prefix in the address pool view. The DHCPv6 PD

 Copyright © Huawei Technologies Co., Ltd.

client divides the obtained prefix into prefixes of subnet segments and sends an RA message on the network segment that hosts directly connect to or exchange information with hosts using the DHCPv6 protocol. The RA message contains the prefixes of subnet segments. This enables hosts to automatically configure addresses.

Precautions

- Idle addresses or prefixes are assigned to DHCPv6 clients from the IPv6 address pool. Reserved addresses, conflicted addresses, and used addresses cannot be assigned to DHCPv6 clients. Reserved addresses include unspecified addresses, multicast addresses, loopback addresses, link-local addresses, NSAP addresses, and anycast addresses (defined in RFC 2526).
- The agent prefix cannot be overlapped.
- The agent prefix cannot be overlapped with the address prefix.
- The agent prefix cannot be overlapped with the prefix statically specified by a certain user.
- When the prefix pool is deleted, all prefix leases are deleted.
- Only one agent prefix can be configured for an address pool.

Example

Configure the agent prefix of the DHCPv6 server as fc00:1::/30 for the address pool pool1, set the prefix length to 42 and the lifetime to infinite.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] prefix-delegation fc00:1::/30 42 life-time infinite infinite
```

Related Topics

8.9.14 dhcpv6 pool

8.9.50 reset dhcpv6 client statistics

Function

The **reset dhcpv6 client statistics** command clears DHCPv6 message statistics on the DHCPv6 client.

Format

reset dhcpv6 client statistics [**interface** *interface-type interface-number*]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears DHCPv6 message statistics on a specified interface. If no interface is specified, all message statistics on the DHCPv6 client are cleared.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command applies to the DHCPv6 client. Collecting statistics about the DHCPv6 messages sent and received within a specified period helps you locate DHCPv6 faults. Before collecting new statistics, run the **reset dhcpv6 client statistics** [**interface** *interface-type interface-number*] command to clear the existing message statistics. After clearing existing statistics, run the **display dhcpv6 client statistics** [**interface** *interface-type interface-number*] command to view latest message statistics.

Example

Clear message statistics on the DHCPv6 client.

```
<Huawei> reset dhcpv6 client statistics
```

8.9.51 reset dhcpv6 pool

Function

The **reset dhcpv6 pool** command clears the IPv6 address pool configured on the device.

Format

reset dhcpv6 pool *pool-name* [**allocated** { **address** | **prefix** } | **binding** [*duid*] | **conflict address** | *ipv6-address* [**to** *ipv6-address*] | *ipv6-prefix/prefix-length*]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
pool *pool-name*	Specifies the IPv6 address pool name.	The value is a string of 1 to 31 characters without spaces. The value contains digits, letters, underscores (_), and dots (.).
allocated { **address** | **prefix** }	Deletes IPv6 addresses or IPv6 address prefixes that have been assigned.	-
binding [*duid*]	Deletes addresses that are bound to DUIDs.	The value is a string of 2 to 256 characters in hexadecimal notation. The length of the string is an even.
conflict address	Resets the conflicted IPv6 addresses in the IPv6 address pool.	-
ipv6-address [**to** *ipv6-address*]	Resets IPv6 addresses in the IPv6 address pool. If only one IPv6 address is entered, only the entered IPv6 address is reset.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
ipv6-prefix/prefix-length	Resets IPv6 prefixes in the IPv6 address pool.	The value is a 32-digit hexadecimal number, in the format X:X::X:X/M. The IPv6 address prefix length ranges from 16 to 128

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **reset dhcpv6 pool** command resets the address pool status. If an IPv6 address conflict occurs because two clients use the same IPv6 address, you need to set the IPv6 address pool to idle.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

If a user's IPv6 address is within the IPv6 address range specified when this command is run, the user cannot continue to use the IPv6 address after this command is run, and needs to send an IPv6 address application request again.

The address pool status cannot be restored after this command is run. Therefore, exercise caution when deciding to run this command.

Example

Set the status of all the conflicted IPv6 addresses in the IPv6 address pool mypool to idle.

```
<Huawei> reset dhcpv6 pool mypool conflict address
```

Related Topics

8.9.14 dhcpv6 pool

8.9.52 reset dhcpv6 relay statistics

Function

The **reset dhcpv6 relay statistics** command clears DHCPv6 message statistics on the DHCPv6 relay agent.

Format

reset dhcpv6 relay statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. If no interface is specified, all the DHCPv6 message statistics are cleared. If an interface is specified, DHCPv6 message statistics on the specified interface are cleared.	-

Views

User view

Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

If a device is enabled with the DHCPv6 relay function, the system takes the statistics about DHCPv6 messages passing through the DHCP relay agent. You can use the **reset dhcpv6 relay statistics** command to clear current message statistics on the DHCPv6 relay agent.

Example

Clear the DHCPv6 message statistics on VLANIF 10.

```
<Huawei> reset dhcpv6 relay statistics interface vlanif 10
```

Related Topics

8.9.31 display dhcpv6 relay statistics

8.9.53 reset dhcpv6 server statistics

Function

The **reset dhcpv6 server statistics** command clears DHCPv6 message statistics on the DHCPv6 server.

Format

reset dhcpv6 server statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

If a device is enabled with the DHCPv6 server function, the system takes the statistics about DHCPv6 messages passing through the DHCPv6 server. You can

Copyright © Huawei Technologies Co., Ltd.

use the **reset dhcpv6 server statistics** command to clear current message statistics on the DHCPv6 server.

If no interface is specified, all the DHCPv6 message statistics are cleared. If an interface is specified, DHCPv6 message statistics on the specified interface are cleared.

Example

Clear DHCPv6 message statistics.

```
<Huawei> reset dhcpv6 server statistics
```

Related Topics

8.9.34 display dhcpv6 server

8.9.54 reset dhcpv6 statistics

Function

The **reset dhcpv6 statistics** command clears DHCPv6 packet statistics.

Format

reset dhcpv6 statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Collecting statistics about the DHCPv6 messages sent and received within a specified period helps you locate DHCPv6 faults. Before collecting new statistics, run the **reset dhcpv6 statistics** command to clear the existing message statistics. After clearing existing statistics, run the **display dhcpv6 statistics** command to view latest message statistics.

Example

Clear DHCPv6 packet statistics.

```
<Huawei> reset dhcpv6 statistics
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

8.9.36 display dhcpv6 statistics

8.9.55 sip-domain-name

Function

The **sip-domain-name** command configures the SIP domain name suffix assigned by the DHCPv6 server to a DHCPv6 client.

The **undo sip-domain-name** command deletes the assigned SIP domain name suffix.

By default, no SIP domain name suffix is configured for the DHCPv6 client.

Format

sip-domain-name *sip-domain-name*

undo sip-domain-name *sip-domain-name*

Parameters

Parameter	Description	Value
sip-domain-name	Specifies the SIP domain name suffix assigned to a DHCPv6 client.	The value is a string of 1 to 63 case-insensitive characters without spaces. The value contains letters, digits, underscores (_), and dots (.).

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **sip-domain-name** command is used on DHCPv6 servers. The DHCPv6 server specifies an SIP domain name when allocating IPv6 addresses for clients. You can use the **sip-domain-name** command on the DHCPv6 server to specify a SIP domain name for each global address pool. When allocating IPv6 addresses to clients, the DHCPv6 server also sends the domain name suffixes to the clients.

Precautions

Copyright © Huawei Technologies Co., Ltd.

A maximum of four SIP domain name suffixes can be configured for an IPv6 address pool.

Example

Configure the SIP domain name assigned to the DHCPv6 client as **sip.com** for the address pool **pool1**.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] sip-domain-name sip.com
```

Related Topics

8.9.14 dhcpv6 pool

8.9.56 sip-server (IPv6 address pool view)

Function

The **sip-server** command configures the SIP server address assigned to the DHCPv6 client for the IPv6 address pool.

The **undo sip-server** command deletes the configured SIP server address assigned to the DHCPv6 client from the IPv6 address pool.

By default, no SIP server address is configured for the IPv6 address pool.

Format

sip-server *ipv6-address*

undo sip-server *ipv6-address*

Parameters

Parameter	Description	Value
ipv6-address	SIP server IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

The **sip-server** command is used on DHCPv6 servers. The DHCPv6 server needs to specify the IPv6 address of the SIP server for the address pool so that the DHCPv6 client can be connected to the Internet. The DHCPv6 server specifies the IPv6 address of the SIP server when allocating IPv6 addresses to the clients.

Precautions

- A maximum of two SIP server addresses can be configured for each address pool. The first assigned address functions as the primary address, and the other address functions as a secondary address.
- When multiple SIP servers are specified, you need to run the **sip-server** repeatedly to configure multiple addresses.

Example

Specify fc00:3::1 as the IPv6 address of the SIP server when the assigned IPv6 address belongs to the address pool **global1**.

```
<Huawei> system-view
[Huawei] dhcpv6 pool global1
[Huawei-dhcpv6-pool-global1] sip-server fc00:3::1
```

Related Topics

8.9.14 dhcpv6 pool

8.9.57 sntp-server

Function

The **sntp-server** command configures the SNTP server IPv6 address assigned to the DHCPv6 client for the IPv6 address pool.

The **undo sntp-server** command deletes the configured SNTP server IPv6 address assigned to the DHCPv6 client from the IPv6 address pool.

By default, no SNTP server IPv6 address is configured for the IPv6 address pool.

Format

sntp-server *ipv6-address*

undo sntp-server *ipv6-address*

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of an SNTP server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Copyright © Huawei Technologies Co., Ltd.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **sntp-server** command is used on DHCPv6 servers. The DHCPv6 server needs to specify the IPv6 address of the SNTP server for the IPv6 address pool so that the DHCPv6 client can be connected to the Internet. The DHCPv6 server specifies the IPv6 address of the SNTP server when allocating IPv6 addresses to the clients. After the clients receive the IPv6 address of the SNTP server, the clients synchronize the system time with the specified SNTP server.

Precautions

- A maximum of two SNTP server addresses can be configured for each IPv6 address pool. The first assigned address functions as the primary address, and the other address functions as a secondary address.
- When multiple SNTP servers are specified, you need to run the **sntp-server** command repeatedly to configure multiple addresses.

Example

Specify fc00:1::1 as the IPv6 address of the SNTP server when IPv6 addresses in the address pool **global1** are assigned.

```
<Huawei> system-view
[Huawei] dhcpv6 pool global1
[Huawei-dhcpv6-pool-global1] sntp-server fc00:1::1
```

Related Topics

8.9.14 dhcpv6 pool

8.9.58 static-bind address

Function

The **static-bind address** command statically binds an IPv6 address to the client DUID in the DHCPv6 address pool view.

The **undo static-bind address** command deletes the statically bound entries between the IPv6 address and the client DUID in the DHCPv6 address pool view.

By default, no IPv6 address is bound to the client DUID in the address pool view.

Format

static-bind address [*prefix-name*] *ipv6-address* **duid** *client-duid* [**iaid** *iaid*] [**life-time** { *valid-lifetime* | **infinite** } { *preferred-lifetime* | **infinite** }]

 Copyright © Huawei Technologies Co., Ltd.

undo static-bind address [*prefix-name*] *ipv6-address*

Parameters

Parameter	Description	Value
prefix-name	Specifies the name of an IPv6 address prefix name.	The value is a string of 1 to 63 case-sensitive characters without spaces.
ipv6-address	Specifies the IPv6 address statically bound to an address pool.	The 128-bit IPv6 address is divided into eight groups. Each group contains four hexadecimal digits. The format is X:X:X:X:X:X:X:X.
duid *client-duid*	Configures the DUID of the DHCPv6 client that is statically bound to the IPv6 address.	The value is a string of 2 to 256 characters in hexadecimal notation. The length of the string is an even.
iaid *iaid*	Specifies IA identifier value.	The value is an integer that ranges from 1 to 4294967295.
life-time	Specifies the lifetime of the bound entries.	-
valid-lifetime	Specifies the valid lifetime of the bound entries.	The value is an integer that ranges from 60 to 172799999, in seconds. The default value is 172800, that is two days.
preferred-lifetime	Specifies the preferred lifetime of the bound entries.	The value is an integer that ranges from 60 to 172799999, in seconds. The default value is 86400, that is one day.
infinite	Sets the lifetime of the bound entries to infinite.	-

Views

IPv6 address pool view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The **static-bind address** command is used on DHCPv6 servers. If some special clients need to be statically assigned with fixed IPv6 addresses, bind the DUIDs of these clients to the IPv6 addresses. When receiving a request from a special client for requesting an IPv6 address, a DHCPv6 server assigns the fixed IPv6 address bound to the client DUID to this client.

Prerequisites

1. An address pool has been created by using the **dhcpv6 pool** command.
2. Bind an IPv6 address prefix to an address pool by using the **address prefix**

Example

Bind the IPv6 address fc00:1::2 with the client with DUID abcdef in address pool pool1 and set the lifetime to infinite.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] address prefix fc00:1::/64
[Huawei-dhcpv6-pool-pool1] static-bind address fc00:1::2 duid abcdef life-time infinite infinite
```

Related Topics

8.9.14 dhcpv6 pool

8.9.1 address prefix

8.9.59 static-bind prefix

Function

The **static-bind prefix** command statically binds an IPv6 address prefix to the DHCPv6 PD client in the DHCPv6 address pool view.

The **undo static-bind prefix** command unbinds the IPv6 address prefixes from the DHCPv6 PD clients in the DHCPv6 address pool view.

By default, no IPv6 address prefix is bound to the DHCPv6 PD client in the address pool view.

Format

static-bind prefix *ipv6-prefix/ipv6-prefix-length* **duid** *client-duid* [**iaid** *iaid-value*] [**life-time** { *valid-lifetime* | **infinite** } { *preferred-lifetime* | **infinite** }]

undo static-bind prefix *ipv6-prefix/ipv6-prefix-length*

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ipv6-prefix/ipv6-prefix-length	Specifies the IPv6 address prefix that is statically bound to an address pool.	The value is a 32-digit hexadecimal number, in the format X:X::X:X/M.
duid *client-duid*	Specifies the DUID of the DHCPv6 PD client that is statically bound to the IPv6 address prefix.	The value is a string of 2 to 256 characters in hexadecimal notation. The length of the string is an even.
iaid *iaid-value*	Specifies the IAID of the DHCPv6 PD client that is statically bound to the IPv6 address prefix.	The value is an integer that ranges from 1 to 4294967295.
life-time	Specifies the lifetime of the bound entries.	-
valid-lifetime	Specifies the valid lifetime.	The value is an integer that ranges from 60 to 172799999, in seconds. The default value is 172800, that is two days.
preferred-lifetime	Specifies the preferred lifetime. The preferred lifetime cannot exceed the valid lifetime.	The value is an integer that ranges from 60 to 172799999, in seconds. The default value is 86400, that is one day.
infinite	Sets the lifetime to infinite. When the preferred lifetime is set to infinite, the valid lifetime must be set to infinite.	-

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

The **static-bind prefix** command is used on DHCPv6 PD servers. If some special DHCPv6 PD clients need to be statically assigned with fixed IPv6 address prefixes, bind the DUIDs and IAIDs of these clients to the IPv6 address prefixes. When receiving a request for applying for an IP address prefix from a special DHCPv6 PD client, a DHCPv6 PD server assigns the fixed IPv6 address prefix bound to the DUIDs and IAIDs to this client.

Prerequisites

An address pool has been created by using the **dhcpv6 pool** command.

Precautions

- When assigning addresses for DHCPv6 PD clients, bind the address prefix to the DUID of the client. The IAID of the client cannot be specified.
- The statically bound prefix cannot be overlapped with the prefix that is configured using the **prefix-delegation** command.

Example

Bind the IPv6 address prefix fc00:1::/64 to the DHCPv6 PD client with DUID abcdef and IAID 12 in address pool pool1 and set the lifetime of the binding entries to infinite.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] static-bind prefix fc00:1::/64 duid abcdef iaid 12 life-time infinite infinite
```

Related Topics

8.9.14 dhcpv6 pool

8.9.49 prefix-delegation

8.9.60 suboption

Function

The **suboption** command configures vendor-defined DHCPv6 sub-options.

The **undo suboption** command deletes vendor-defined DHCPv6 sub-options.

By default, no vendor-defined DHCPv6 sub-option is configured.

Format

suboption *suboption-code* { **address** *ipv6-address* &<1-4> | **ascii** *ascii-string* | **hex** *hex-string* }

undo suboption *suboption-code*

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
suboption-code	Specifies the code of the vendor-defined DHCPv6 sub-options.	The value is an integer that ranges from 1 to 65535.
address *ipv6-address*	Specifies the vendor-defined option code as the IPv6 address type.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
ascii *ascii-string*	Specifies the vendor-defined option code as an ASCII character string.	The value is a string of 1 to 255 characters. The value contains digits, letters, underscores (_), and dots (.).
hex *hex-string*	Specifies the vendor-defined option code as a hexadecimal string.	The value is a hexadecimal numeral string with an even number of characters (such as aa or aaaa). The even number ranges from 2 to 128.

Views

Vendor-defined mode view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **suboption** command is used on DHCPv6 servers. Run the **vendor-specific** command to enter the vendor-defined mode. In this mode, configure the vendor-defined DHCPv6 options. The DHCPv6 device can carry vendor-defined options such as the TFTP server name and address, and the configuration file of the device.

The **suboption** command configures vendor-defined DHCPv6 sub-options.

Precautions

A maximum of 16 vendor-defined sub-options can be configured in the vendor-defined mode view.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set Huawei-defined sub-option 10 to fc00:1::5 in the IPv6 address pool pool1 view.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] vendor-specific 2011
[Huawei-dhcpv6-pool-pool1-vs-2011] suboption 10 address fc00:1::5
```

Related Topics

8.9.14 dhcpv6 pool
8.9.61 vendor-specific

8.9.61 vendor-specific

Function

The **vendor-specific** command configures vendor-defined options for the IPv6 address pool and enter the vendor-defined mode view.

The **undo vendor-specific** command deletes vendor-defined options configured for the IPv6 address pool.

By default, no vendor-defined option is configured.

Format

vendor-specific *vendor-id*

undo vendor-specific *vendor-id*

Parameters

Parameter	Description	Value
vendor-id	Indicates the ID of the vendor, which is assigned by the IANA. 2011 is the identifier for Huawei.	The value is an integer that ranges from 1 to 4294967295.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

The **vendor-specific** command is used on DHCP servers. You can use the **vendor-specific** command to enter the vendor-defined mode. In this mode, you can configure the vendor-defined DHCPv6 options. The DHCPv6 device can carry vendor-defined options such as the TFTP server name and address, and the configuration file of the device.

Precautions

A maximum of eight vendor-defined modes are configured for one IPv6 address pool. 2011 is the identifier for Huawei.

Example

Configure Huawei-defined options for the IPv6 address pool pool1.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] vendor-specific 2011
[Huawei-dhcpv6-pool-pool1-vs-2011]
```

Related Topics

8.9.14 dhcpv6 pool

8.9.62 import all (IPv6 address pool view)

Function

The **import all** command enables the device to dynamically assign configurations of the DNS server and SNTP server to DHCPv6 clients.

The **undo import all** command disables the device from dynamically assigning configurations of the DNS server and SNTP server to DHCPv6 clients.

By default, the device does not dynamically assign configurations of the DNS server and SNTP server to DHCPv6 clients.

Format

import all interface *interface-type interface-number*

undo import all

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the interface to which a client connects. • *interface-type* specifies the type of the interface. • *interface-number* specifies the number of the interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **import all** command is used on the DHCPv6 server. You can run this command to configure the DHCPv6 server to automatically assign configurations of the DNS server and SNTP server allocated by the carrier to DHCPv6 clients.

Prerequisites

An IPv6 address pool has been created using the **8.9.14 dhcpv6 pool** command.

Example

Configure the device to dynamically assign configurations of the DNS server and SNTP server to DHCPv6 clients.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] import all interface vlanif 100
```

8.10 IPv6 DNS Configuration Commands

8.10.1 dns proxy ipv6 enable

Function

The **dns proxy ipv6 enable** command enables IPv6 DNS proxy.

The **undo dns proxy ipv6 enable** command disables IPv6 DNS proxy.

By default, IPv6 DNS proxy is disabled.

Format

dns proxy ipv6 enable

undo dns proxy ipv6 enable

Parameters

None

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

IPv6 DNS proxy is used to forward DNS requests and reply packets between the IPv6 DNS client and DNS server. The IPv6 DNS client sends a DNS request packet to the device on which IPv6 DNS proxy is enabled. The device sends the request packet to the DNS server and sends the reply packet to the IPv6 DNS client. The device functions as the IPv6 DNS proxy to provide services of the DNS server. Users do not need to interact with the DNS server directly. This function simplifies route deployment and improves performance and security of the DNS server.

Example

Enable IPv6 DNS proxy.

```
<Huawei> system-view
[Huawei] dns proxy ipv6 enable
```

8.10.2 dns relay ipv6 enable

Function

The **dns relay ipv6 enable** command enables IPv6 DNS relay.

The **undo dns relay ipv6 enable** command disables IPv6 DNS relay.

By default, IPv6 DNS relay is disabled.

Format

dns relay ipv6 enable

undo dns relay ipv6 enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

IPv6 DNS relay is used to forward DNS requests and reply packets between the IPv6 DNS client and DNS server. The IPv6 DNS client sends a DNS request packet to the device on which IPv6 DNS relay is enabled. The device sends the request packet to the DNS server and sends the reply packet to the IPv6 DNS client. The

 Copyright © Huawei Technologies Co., Ltd.

device functions as the IPv6 DNS relay to provide services of the DNS server. Users do not need to interact with the DNS server directly. This function simplifies route deployment and improves performance and security of the DNS server.

Example

Enable IPv6 DNS relay.

```
<Huawei> system-view
[Huawei] dns relay ipv6 enable
```

8.10.3 display dns ipv6 dynamic-host

Function

The **display dns ipv6 dynamic-host** command displays IPv6 dynamic DNS entries saved in the cache.

Format

display dns ipv6 dynamic-host [*domain-name* | **a6**]

Parameters

Parameter	Description	Value
domain-name	Displays IPv6 entries specified the domain name suffix.	The value must be an existing domain name suffix.
a6	Displays IPv6 entries specified A6 query type.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After dynamic domain name resolution is completed, you can run the **display dns ipv6 dynamic-host** command to check dynamic IPv6 DNS entries in the domain name cache.

Example

Display the IPv6 dynamic DNS entries saved in the cache.

```
<Huawei> display dns ipv6 dynamic-host
Host                            TTL       Type   Address
```

 Copyright © Huawei Technologies Co., Ltd.

```
www.huawei.com                  3411      IPv6   FC00:1::1

Total  :  1
```

Table 8-107 Description of the **display dns ipv6 dynamic-host** command output

Item	Description
Host	Domain name.
TTL	Time left before dynamic DNS entries saved in the domain name cache will be aged out, in seconds.
Type	Dynamic DNS entry type.
Address	IPv6 address in a dynamic cache entry.

Related Topics

8.10.10 reset dns ipv6 dynamic-host

8.10.4 display dns ipv6 forward table

Function

The **display dns ipv6 forward table** command displays the DNS forwarding table.

Format

display dns ipv6 forward table [**source-ip** *ipv6-address*]

Parameters

Parameter	Description	Value
source-ip *ipv6-address*	Specifies the source IPv6 address in query messages.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X. Two or more consecutive zeros in the address can be replaced by "::".

Views

All views

Default Level

1: Monitoring level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After IPv6 DNS proxy or IPv6 DNS relay is enabled, you can run the **display dns ipv6 forward table** command to view the DNS forwarding table of IPv6 addresses. When the IPv6 DNS proxy or IPv6 DNS relay is attacked, the DNS forwarding table will be full. As a result, new DNS entries cannot be queried. You can run the **reset dns ipv6 forward table** command to delete all DNS entries.

Example

Display the IPv6 DNS forwarding table.

```
<Huawei> display dns ipv6 forward table
Domain name            : www.ipv6.com
Source IPv6 address    : FC00:1::5
Source port            : 49154
Source packet id       : 5
Forward packet id      : 0
Query type             : 28
VPN-Instance           : vpna
```

Table 8-108 Description of the **display dns ipv6 forward table** command output

Item	Description
Domain name	Domain name.
Source IPv6 address	Source IPv6 address of a query message.
Source port	Source port of a query message.
Source packet id	ID of a query message.
Forward packet id	ID of the forwarded packet, which corresponds to the ID of the query message.
Query type	Query type • 28: AAAA query • 38: A6 query
VPN-Instance	Name of the VPN instance that the DNS client belongs to.

Related Topics

8.10.11 reset dns ipv6 forward table

8.10.5 display ipv6 host

Function

The **display ipv6 host** command displays the IPv6 static DNS table.

Copyright © Huawei Technologies Co., Ltd.

Format

display ipv6 host

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After running the **ipv6 host** command to configure IPv6 static DNS entries, you can run this command to check whether mappings between host names and IPv6 addresses are correct.

Example

Display the IPv6 static DNS table.

```
<Huawei> display ipv6 host
Host                 Age        Flags    IPv6Address (es)
www.huawei.com       0          static   FC00:1::8
www.sohu.com         0          static   FC00:1::9
```

Table 8-109 Description of the **display ipv6 host** command output

Item	Description
Host	Host name.
Age	Aging time. The value 0 indicates that the entry is not aged out.
Flags	DNS table identifiers. The value static indicates a static domain name.
IPv6Address (es)	IPv6 address mapping the domain name.

Related Topics

8.10.9 ipv6 host

Copyright © Huawei Technologies Co., Ltd.

8.10.6 dns server ipv6

Function

The **dns server ipv6** command configures the IPv6 address for the DNS server that resolves dynamic domain names.

The **undo dns server ipv6** command deletes the configured IPv6 address for DNS server.

By default, no IPv6 address is configured for the DNS server that resolves dynamic domain names.

Format

dns server ipv6 *ipv6-address* [*interface-type interface-number*]

undo dns server ipv6 [*ipv6-address* [*interface-type interface-number*]]

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address for a DNS server.	The value has 128 bits. It is represented as eight groups of four hexadecimal digits with the groups being separated by colons, in the format of X:X:X:X:X:X:X:X.
interface-type interface-number	Specifies the type and number of an outbound interface that communicates with the DNS server.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The IPv6 DNS client must work with the DNS server to implement dynamic domain name resolution. You can run the **dns server ipv6** command to specify the

 Copyright © Huawei Technologies Co., Ltd.

IPv6 address of the DNS server. The IPv6 DNS client sends requests to the specified DNS server for domain name resolution.

Precautions

- The IPv6 address of the DNS server must be a global unicast address or link-local address.
  - If a link-local address is configured as the IPv6 address of the DNS server, specify the outbound interface for communicating with the DNS server.
  - If a global unicast address is configured as the IPv6 address of the DNS server, do not specify the outbound interface for communicating with the DNS server.
- The device supports a maximum of six IPv6 addresses of the DNS server.

Example

Configure the IPv6 address of the DNS server to fc00:1::1.

```
<Huawei> system-view
[Huawei] dns server ipv6 fc00:1::1
```

8.10.7 dns server ipv6 source-ip

Function

The **dns server ipv6 source-ip** command configures the source IPv6 address for the local end functioning as the DNS client to communicate with the IPv6 DNS server.

The **undo dns server ipv6 source-ip** command deletes the source IPv6 address for the local end functioning as the DNS client to communicate with the IPv6 DNS server.

By default, no source IPv6 address is configured for the local end functioning as the DNS client to communicate with the IPv6 DNS server.

Format

dns server ipv6 source-ip *ipv6-address*

undo dns server ipv6 source-ip

Parameters

Parameter	Description	Value
ipv6-address	Specifies the source IPv6 address of the local device.	The value has 128 bits. It is represented as eight groups of four hexadecimal digits with the groups being separated by colons, in the format of X:X:X:X:X:X:X:X.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the source IPv6 address of the local device is specified, the device uses the specified source IPv6 address to communicate with the IPv6 DNS server to ensure the security check. The DNS server returns the request for a domain name to the local device along the specified route. If no source IPv6 address is configured, the DNS client needs to select a source IPv6 address according to the destination address each time it sends an IPv6 DNS request.

Precautions

To make the command take effect, pay attention to the following points:

- If the DNS server has only one reachable route containing a specified destination IPv6 address to the device, you need to specify the source IPv6 address in the DNS query request sent from the device to the DNS server.
- Ensure that the source IPv6 address is the IPv6 address of an interface or logical interface on the device, and there are reachable routes between the interface and the DNS server.
- Ensure that the source IPv6 address and the IPv6 address of the DNS server are on the same VPN or public network.

Example

Configure the source IPv6 address of the local device to fc00:1::1.

```
<Huawei> system-view
[Huawei] dns server ipv6 source-ip fc00:1::1
```

8.10.8 dns spoofing ipv6

Function

The **dns spoofing ipv6** command enables IPv6 DNS spoofing and specifies an IPv6 address in response messages.

The **undo dns spoofing ipv6** command disables IPv6 DNS spoofing.

By default, IPv6 DNS spoofing is disabled.

Format

dns spoofing ipv6 *ipv6-address*

 Copyright © Huawei Technologies Co., Ltd.

undo dns spoofing ipv6

Parameters

Parameter	Description	Value
ipv6-address	Specifies an IPv6 address in response messages.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the DNS server address or route to the DNS server is not configured on the DNS proxy or relay, you can enable DNS spoofing on the device to spoof a response message with the configured IPv6 address. Currently, IPv6 DNS spoofing takes effect for only AAAA query (IPv6 address query based on domain names) and A6 query.

Prerequisites

DNS relay or DNS proxy has been enabled using the **8.4.17 dns relay enable** or **8.4.15 dns proxy enable** command in the system view.

Precautions

If you run the **dns spoofing ipv6** command multiple times, only the latest configuration takes effect.

Example

Enable DNS spoofing and specify the IPv6 address in response messages as fc00:1::8.

```
<Huawei> system-view
[Huawei] dns spoofing ipv6 fc00:1::8
```

Related Topics

8.4.17 dns relay enable

8.4.15 dns proxy enable

 Copyright © Huawei Technologies Co., Ltd.

8.10.9 ipv6 host

Function

The **ipv6 host** command configures IPv6 static DNS entries.

The **undo ipv6 host** command deletes IPv6 static DNS entries.

By default, no IPv6 static DNS entry is configured.

Format

ipv6 host *host-name ipv6-address*

undo ipv6 host *host-name* [*ipv6-address*]

Parameters

Parameter	Description	Value
host-name	Specifies the host name.	The value is a string of 1 to 255 case-sensitive characters without any space. The value must contain at least one letter, and can consist of letters, digits, hyphens (-), dots (.), and underscores (_).
ipv6-address	Specifies the IPv6 address mapping the host name.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When device functions as a DNS proxy or DNS client and requests the IPv6 address mapping a domain name, the device searches for the specified domain

Copyright © Huawei Technologies Co., Ltd.

name in the static DNS table to obtain the mapping IPv6 address. The **ipv6 host** command configures IPv6 static DNS entries.

Precautions

Each domain name supports a maximum of 8 IPv6 addresses.

Example

Configures IPv6 static DNS entries mapping the host named **www.huawei.com**.

```
<Huawei> system-view
[Huawei] ipv6 host www.huawei.com fc00:1::8
```

Related Topics

8.10.5 display ipv6 host

8.10.10 reset dns ipv6 dynamic-host

Function

The **reset dns ipv6 dynamic-host** command clears IPv6 dynamic DNS entries saved in the cache.

Format

reset dns ipv6 dynamic-host

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

IPv6 dynamic DNS entries cannot be restored after being deleted. Confirm the action before you run the command.

Example

Clear IPv6 dynamic DNS entries saved in the cache.

```
<Huawei> reset dns ipv6 dynamic-host
```

Related Topics

8.10.3 display dns ipv6 dynamic-host

 Copyright © Huawei Technologies Co., Ltd.

8.10.11 reset dns ipv6 forward table

Function

The **reset dns ipv6 forward table** command clears entries in the IPv6 DNS forward table.

Format

reset dns ipv6 forward table [**source-ip** *ipv6-address*]

Parameters

Parameter	Description	Value
source-ip *ipv6-address*	Specifies the source IPv6 address in query messages.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.

Views

User view

Default Level

3: Management level

Usage Guidelines

When the DNS proxy or relay is attacked, the DNS table will be full. As a result, new DNS entries cannot be queried. You can run the **display dns ipv6 forward table** command to view the DNS table, and run the **reset dns ipv6 forward table** command to clear entries in the DNS table.

Example

Clear DNS entries in the DNS table on the IPv6 DNS proxy or DNS relay.

```
<Huawei> reset dns ipv6 forward table
```

Related Topics

8.10.4 display dns ipv6 forward table

8.11 IPv6 over IPv4 Tunnel Configuration Commands

Copyright © Huawei Technologies Co., Ltd.

8.11.1 destination

Function

The **destination** command specifies the destination IP address of a tunnel interface.

The **undo destination** command deletes the destination IP address of a tunnel interface.

By default, no destination address is configured.

Format

destination [**vpn-instance** *vpn-instance-name*] *dest-ip-address*

undo destination

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance that the destination address of a tunnel belongs to. When the tunnel interface uses GRE tunnel or IPSec tunnel, you can specify **vpn-instance** *vpn-instance-name*.	The value is the name of an existing VPN instance.
dest-ip-address	Specifies the destination IP address of a tunnel interface.	The value is in dotted decimal notation.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring a GRE, IPv4 over IPv6, IPSec, MPLS TE, manual IPv6 over IPv4 tunnel, create a tunnel interface. After a tunnel interface is created, run the **destination** command to specify the destination IP address for the tunnel interface.

When using the **destination** command on a PE to specify the destination address of a GRE tunnel bound for a CE, you need to set **vpn-instance** *vpn-instance-name* in the command to specify the name of the VPN instance to which the destination address belongs.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

A tunnel interface has been created using the **interface tunnel** command, and the encapsulation mode is set to GRE, IPSec, MPLS TE, IPv4 over IPv6, or IPv6 over IPv4 of manual mode using the **tunnel-protocol** command.

Precautions

Two or more GRE tunnel interfaces in a system can have the same source address and same destination address. The system uses GRE keys to identify these GRE tunnel interfaces. Normally, two tunnel interfaces in a system cannot have the same encapsulation mode, source address, and destination address.

Two tunnel interfaces with the same encapsulation mode, source address, and destination address cannot be configured simultaneously.

On the IPSec, IPv6 over IPv4, IPv4 over IPv6, or GRE tunnel, the destination address of the local tunnel interface is the source address of the remote tunnel interface by the **source** command, and the source address of the local tunnel interface is the destination address of the remote tunnel interface.

Example

Set the destination address of the GRE tunnel Tunnel 0/0/1 to 10.1.1.1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol gre
[Huawei-Tunnel0/0/1] destination 10.1.1.1
```

Set the destination address of the GRE tunnel Tunnel 0/0/0 to 10.1.1.1 that belongs to vpn1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre
[Huawei-Tunnel0/0/0] destination vpn-instance vpn1 10.1.1.1
```

Related Topics

12.3.10 interface tunnel
8.11.3 source
8.11.4 tunnel-protocol

8.11.2 interface tunnel

Function

The **interface tunnel** command creates a tunnel interface.

The **undo interface tunnel** command deletes the configured tunnel interface.

By default, no tunnel interface is configured.

Format

interface tunnel *interface-number*

undo interface tunnel *interface-number*

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-number	Specifies the number of the tunnel interface.	The value is in the format slot ID/subcard ID/port sequence number and varies according to the device type.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To forward data packet over tunnels (for example, VPN tunnels), ensure that the tunnel has been created. The system supports the following types of tunnels:

- LSP (Static LSP, BGP LSP, LDP LSP)
- MPLS TE
- IPSec
- GRE
- IPv6 over IPv4
- IPv4 over IPv6

You must use the **interface tunnel** command to create a tunnel interface when creating a tunnel except for LSP tunnels.

Precautions

After a tunnel interface is created, you need to configure an IP address and encapsulation type for the tunnel interface.

To save IP addresses, run the **ip address unnumbered** command to configure the tunnel interface to borrow an IP address of another interface.

The **tunnel-protocol** command configures an encapsulation protocol for the tunnel interface.

Tunnel interface numbers are valid on the local device only. You can configure different numbers for the tunnel interfaces

Example

Create a tunnel interface.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1]
```

8.11.3 source

Function

The **source** command configures the source address or source interface of the tunnel.

The **undo source** command deletes the configured source address or source interface.

The source address and source interface of a tunnel are not specified by default.

Format

source { [**vpn-instance** *vpn-instance-name*] *source-ip-address* | *interface-type interface-number* }

undo source

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance that the source address of a tunnel belongs to. **NOTE** You can specify the parameter only when the encapsulation mode of a tunnel interface is set to IPSec or mGRE.	The value is the name of an existing VPN instance.
source-ip-address	Specifies the source address of a tunnel interface. If a tunnel interface works in IPv4-IPv6 mode, specify an IPv6 address as the source address of the tunnel interface.	The IPv4 address is in dotted decimal notation. The IPv6 address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
interface-type interface-number	Specifies the type and the number of the source interface of the tunnel.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Tunnel interface view, Tunnel-Template interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring a tunnel, you must create a tunnel interface. After a tunnel interface is created, run the **source** command to specify the source IP address for the tunnel interface.

Prerequisites

A tunnel interface has been created using the **interface tunnel** command, and the encapsulation mode is set to GRE, IPSec, IPv4 over IPv6, or IPv6 over IPv4 of manual mode using the **tunnel-protocol** command.

Precautions

Two tunnel interfaces with the same encapsulation mode, source address, and destination address cannot be configured simultaneously.

IPv6 over IPv4, IPv4 over IPv6, and GRE tunnels are bidirectional tunnels. The source address of the local tunnel interface is the destination address of the remote tunnel interface by the **destination** command, and the destination address of the local tunnel interface is the source address of the remote tunnel interface.

Two or more tunnel interfaces that use the same encapsulation protocol cannot be configured with the same source and destination addresses. Two or more GRE tunnel interfaces in a system can have the same source address and same destination address. The system uses GRE keys to identify these GRE tunnel interfaces. When two or more tunnel interfaces on a P2MP tunnel are configured with the same source address, run the **gre key** command to set the key number of each tunnel interface.

You can also specify VPN instance parameters while specifying the source address for an IPSec tunnel or an mGRE tunnel in IPSec/mGRE over VPN scenarios.

Example

Set the tunnel type of Tunnel0/0/1 to IPv6 over IPv4 manual tunnel and configure the source IP address of Tunnel0/0/1 as 10.1.1.1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol ipv6-ipv4
[Huawei-Tunnel0/0/1] source 10.1.1.1
```

Configure Tunnel0/0/2 of mGRE and use Loopback0 address as the interface address.

```
<Huawei> system-view
[Huawei] interface loopback 0
[Huawei-LoopBack0] ip address 10.2.1.1 32
[Huawei-LoopBack0] quit
[Huawei] interface tunnel 0/0/2
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-Tunnel0/0/2] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/2] source loopback 0
```

8.11.4 tunnel-protocol

Function

The **tunnel-protocol** command configures the tunnel protocol on a tunnel interface.

The **undo tunnel-protocol** command restores the tunnel protocol to the default configuration.

By default, no tunnel protocol is used on a tunnel interface.

Format

tunnel-protocol { **gre** [**p2mp**] | **ipsec** | **ipv6-ipv4** [**6to4** | **auto-tunnel** | **isatap**] | **ipv4-ipv6** | **mpls te** | **svpn** [**p2p** | **p2mp**] | **none** }

undo tunnel-protocol

Parameters

Parameter	Description	Value
gre	Indicates that the GRE tunnel protocol is configured on a tunnel interface.	-
gre p2mp	Indicates that the mGRE tunnel protocol is configured on a tunnel interface. If this parameter is not used, the tunnel protocol configured on a tunnel interface is a traditional point-to-point GRE.	-
ipsec	Indicates that the IPSec tunnel protocol is configured on a tunnel interface.	-
ipv4-ipv6	Indicates that the IPv4 to IPv6 tunnel protocol is configured on a tunnel interface.	-
ipv6-ipv4	Configures the tunnel protocol of the tunnel interface as ipv6-ipv4 and uses a manual IPv6 over IPv4 tunnel.	-
ipv6-ipv4 6to4	Indicates that the IPv6 to IPv4 tunnel protocol is configured on a tunnel interface using 6to4.	-
ipv6-ipv4 auto-tunnel	Configures the tunnel protocol of the tunnel interface as ipv6-ipv4 and uses an automatic IPv6 over IPv4 tunnel.	-
ipv6-ipv4 isatap	Indicates that the IPv6 to IPv4 tunnel protocol is configured on a tunnel interface using isatap.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
mpls te	Indicates that the MPLS TE tunnel protocol is configured on a tunnel interface. **NOTE** The AR100&AR120&AR150&AR160&AR200 does not support this parameter.	-
svpn [**p2p** | **p2mp**]	Indicates that the SVPN tunnel protocol is configured on a tunnel interface. • **p2p**: indicates the P2P SVPN tunnel protocol. • **p2mp**: indicates the P2MP SVPN tunnel protocol.	-
none	Indicates that no tunnel protocol is configured on a tunnel interface.	-

Views

Tunnel interface view, Tunnel-Template interface view

NOTE

The tunnel template interface view supports the **ipsec** and **none** parameters only.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a tunnel interface using the **interface tunnel** command, run the **tunnel-protocol** command to configure the tunnel encapsulation mode for the tunnel interface.

The following tunnel encapsulation modes are available:

- GRE: encapsulates packets of some network layer protocols such as IP or IPX to enable these encapsulated packets to be transmitted on networks running other protocols such as IP. When the **p2mp** parameter is specified following **gre**, you can set the tunnel encapsulation mode to P2MP GRE. The destination address of a P2MP GRE tunnel does not need to be manually configured. Instead, the destination address of this tunnel can either be defined by a protocol (for example, NHRP in a DSVPN scenario) or be dynamically learned.
- IPSec: protects the security of data transmitted on the Internet by establishing tunnels using the IPSec protocol.
- IPv4-IPv6: creates tunnels on the IPv6 networks to connect IPv4 isolated sites so that IPv4 isolated sites can access other IPv4 networks through the IPv6 public network.

 Copyright © Huawei Technologies Co., Ltd.

- IPv6-IPv4: creates tunnels on the IPv4 networks to connect IPv6 isolated sites so that IPv6 packets can be transmitted on IPv4 networks.
- MPLS TE: integrates the MPLS technology with traffic engineering. It can reserve resources by setting up LSP tunnels for a specified path in an attempt to avoid network congestion and balance network traffic.
- SVPN: binds multiple WAN access lines to provide high bandwidth and highly reliable networks for customers.
  - When the SVPN mode is set to Hub-Spoke, specify **p2p** on the Spoke and **p2mp** on the hub when configuring a tunnel protocol.
  - When the SVPN mode is set to Lone Ranger, you must not specify **p2p** or **p2mp**.

Precautions

- The **none** mode indicates the initial configuration, that is, no tunnel encapsulation mode is configured. In practice, you must select another tunnel encapsulation mode.
- You must configure the tunnel encapsulation mode before setting the source IP address or other parameters for a tunnel interface. Changing the encapsulation mode of a tunnel interface deletes other parameters of the tunnel interface. When an SVPN proposal is bound to a tunnel interface, you cannot modify the tunnel encapsulation mode.

Example

Set the tunnel encapsulation mode of Tunnel0/0/2 to mGRE.
```
<Huawei> system-view
[Huawei] interface tunnel 0/0/2
[Huawei-Tunnel0/0/2] tunnel-protocol gre p2mp
```

Set the tunnel encapsulation mode of Tunnel0/0/2 to GRE.
```
<Huawei> system-view
[Huawei] interface tunnel 0/0/2
[Huawei-Tunnel0/0/2] tunnel-protocol gre
```

Related Topics

12.3.10 interface tunnel

8.12 IPv4 over IPv6 Tunnel Configuration Commands

8.12.1 display interface tunnel

Function

The **display interface tunnel** command displays details of the tunnel interface.

Format

display interface tunnel [*interface-number* | **main**]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-number	Specifies the number of the tunnel interface. If this parameter is not specified, the command displays information about all tunnel interfaces.	The value must be the number a tunnel interface that has been created.
main	Displays status and traffic statistics about main interface. The interface has no sub-interfaces. Status and traffic statistics about the interface are displayed whether you specify the main parameter or not.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the details of the tunnel interface.

```
<Huawei> display interface tunnel 0/0/2
Tunnel0/0/2 current state : UP
Line protocol current state : UP
Description:HUAWEI, AR Series, Tunnel0/0/2 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.10.10.1 (GigabitEthernet0/0/1), destination 10.1.1.1
Tunnel protocol/transport GRE/IP, key disabled
keepalive disabled
Checksumming of packets disabled
Current system time: 2012-08-09 18:53:47
    300 seconds input rate 0 bits/sec, 0 packets/sec
    300 seconds output rate 0 bits/sec, 0 packets/sec
    15 seconds input rate 0 bits/sec, 0 packets/sec
    15 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets input,  0 bytes
```

 Copyright © Huawei Technologies Co., Ltd.

```
0 input error
0 packets output,  0 bytes
0 output error
Input bandwidth utilization  : 0%
Output bandwidth utilization : 0%
```

Table 8-110 Description of the display interface tunnel command output

Item	Description
Tunnel0/0/2 current state	Physical layer status of the Tunnel0/0/2 interface: ● UP: The interface is in normal state. ● Administratively DOWN: The network administrator executes the **shutdown** command on the interface. After a tunnel interface is created, its physical layer status is Up.
Line protocol current state	Link protocol status of the Tunnel0/0/2 interface: ● UP: The link layer protocol of the tunnel interface works normally. ● DOWN: The link layer protocol of the tunnel interface is abnormal.
Description	Description of the tunnel interface.
Route Port,The Maximum Transmit Unit is 1500	MTU of tunnel interfaces, which is 1500 bytes by default. Any packet larger than the MTU is fragmented before being sent. If non-fragmentation is configured, the packet is discarded.
Internet protocol processing: disabled	IP protocol is disabled.
Encapsulation is TUNNEL	Encapsulation type of packets on a tunnel interface. Packet encapsulation protects a whole IP packet.
loopback not set	The tunnel interface does not support a loopback test.
Tunnel source 10.10.10.1 (GigabitEthernet0/0/1)	The source address of the tunnel is 10.10.10.1. That is, the IP address of the GigabitEthernet 0/0/1 interface sending packets at the source side is 10.10.10.1.
destination	Destination address of the tunnel.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Tunnel protocol/ transport GRE/IP, key disabled	The tunnel encapsulation protocol is the GRE protocol, and the transport protocol is the IP protocol. Encapsulation protocol types of a tunnel are as follows: ● GRE: indicates Generic Routing Encapsulation. ● IPSec: indicates tunnel mode of IPSec to protect data stream. ● MPLS: encapsulates packets into MPLS packets. ● IPv6 over IPv4: encapsulates IPv6 packets into IPv4 packets. ● IPv4 over IPv6: encapsulates IPv4 packets into IPv6 packets. ● SVPN: encapsulates packets into SVPN packets. ● none: indicates no encapsulation. This is the default mode of the tunnel interface. key disabled: the key word recognition function of GRE is not enabled.
keepalive disabled	The keepalive function of GRE is not enabled.
Checksumming of packets disabled	The check sum function of GRE is not enabled.
300 seconds input rate 0 bits/sec, 0 packets/sec	Rate of bits and packets received on the interface in the last 300 seconds. **NOTE** If the tunnel encapsulation protocol is SVPN, this field is not supported.
300 seconds output rate 0 bits/sec, 0 packets/sec	Rate of bits and packets sent through the interface in the last 300 seconds. **NOTE** If the tunnel encapsulation protocol is SVPN, this field is not supported.
15 seconds input rate 0 bits/sec, 0 packets/sec	Rate of bits and packets received on the interface during the last query period.
15 seconds output rate 0 bits/sec, 0 packets/sec	Rate of bits and packets sent through the interface during the last query period.
0 packets input, 0 bytes 0 input error	Total packets and bytes received on the interface and the total number of defective packets.
0 packets output, 0 bytes 0 output error	Total packets and bytes sent through the interface and the total number of defective packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Input bandwidth utilization	Input bandwidth usage.
Output bandwidth utilization	Output bandwidth usage.

Related Topics

12.3.11 keepalive

8.12.2 tunnel ipv4-ipv6 encapsulation-limit

Function

The **tunnel ipv4-ipv6 encapsulation-limit** command configures the maximum number of times that IPv6 encapsulation can be performed after an IPv4 packet is encapsulated the first time.

The **undo tunnel ipv4-ipv6 encapsulation-limit** command restores the default value.

By default, a maximum of four times of IPv6 encapsulation can be performed on embedded tunnel nodes.

Format

tunnel ipv4-ipv6 encapsulation-limit *encapsulation-limit*

undo tunnel ipv4-ipv6 encapsulation-limit

Parameters

Parameter	Description	Value
encapsulation-limit	Specifies the maximum number of of times for performing IPv6 encapsulation on embedded tunnel nodes.	The value is an integer that ranges from 0 to 255.

Views

System view, tunnel interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The tunnel encapsulation limit is the value of the tunnel encapsulation limit option carried in the destination option extension header in the IPv6 tunnel header.

- If this command is configured in the tunnel interface view, it takes effect only on the current tunnel interface.
- If this command is configured in the system view, it takes effect only on the mobile IPv6 network.

Before running the **tunnel ipv4-ipv6 encapsulation-limit** command in the tunnel interface view, run the **tunnel-protocol ipv4-ipv6** command in the same view to set the tunnel mode to the IPv4 over IPv6 manual tunnel.

The configuration in the system view and the configuration in the tunnel interface view are independent of each other.

When Huawei devices communicate with non-Huawei devices, you must run the **undo tunnel ipv4-ipv6 encapsulation-limit** command to restores the default value.

Example

Set the maximum number of times of IPv6 encapsulation to be performed on the embedded tunnel nodes of the specified IPv4 over IPv6 tunnel to 3.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol ipv4-ipv6
[Huawei-Tunnel0/0/1] tunnel ipv4-ipv6 encapsulation-limit 3
```

Set the maximum number of times of IPv6 encapsulation to be performed on the embedded tunnel nodes of all specified IPv4 over IPv6 tunnels to 3 on the local device.

```
<Huawei> system-view
[Huawei] tunnel ipv4-ipv6 encapsulation-limit 3
```

8.12.3 tunnel ipv4-ipv6 flow-label

Function

The **tunnel ipv4-ipv6 flow-label** command sets the flow label value.

The **undo tunnel ipv4-ipv6 flow-label** command restores the default flow label value.

The default flow label value is 0.

Format

tunnel ipv4-ipv6 flow-label *label-value*

undo tunnel ipv4-ipv6 flow-label

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
label-value	Specifies the flow label value.	The value is an integer that ranges from 0 to 1048575.

Views

Tunnel interface view, system view

Default Level

2: Configuration level

Usage Guidelines

The flow label value of the tunnel refers to the value specified in the flow label field in the IPv6 packet header on the inbound interface of the tunnel.

- If this command is configured in the tunnel interface view, it takes effect only on the current tunnel interface.
- If this command is configured in the system view, it takes effect only on the mobile IPv6 network.

Before running the **tunnel ipv4-ipv6 flow-label** command in the tunnel interface view, run the **tunnel-protocol ipv4-ipv6** command in the same view to set the tunnel mode to the IPv4 over IPv6 manual tunnel.

The configuration in the system view and the configuration in the tunnel interface view are independent of each other.

Example

Set the flow label value of a specified IPv4 over IPv6 tunnel to 10.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol ipv4-ipv6
[Huawei-Tunnel0/0/1] tunnel ipv4-ipv6 flow-label 10
```

8.12.4 tunnel ipv4-ipv6 hop-limit

Function

The **tunnel ipv4-ipv6 hop-limit** command sets the hop limit.

The **undo tunnel ipv4-ipv6 hop-limit** command restores the hop limit to the default value.

By default, the hop limit is 64.

Format

tunnel ipv4-ipv6 hop-limit *hop-limit*

 Copyright © Huawei Technologies Co., Ltd.

undo tunnel ipv4-ipv6 hop-limit

Parameters

Parameter	Description	Value
hop-limit	Specifies the hop limit.	The value is an integer that ranges from 1 to 255.

Views

Tunnel interface view, system view

Default Level

2: Configuration level

Usage Guidelines

Setting the tunnel hop limit can terminate the packet transmission when routing loops occur on the IPv6 tunnel. To make IPv6 tunnel packets reach the egress of the tunnel, the tunnel hop limit cannot be set too small.

- If this command is configured in the tunnel interface view, it takes effect only on the current tunnel interface.
- If this command is configured in the system view, it takes effect only on the mobile IPv6 network.

Before running the **tunnel ipv4-ipv6 hop-limit** command in the tunnel interface view, run the **tunnel-protocol ipv4-ipv6** command in the same view to set the tunnel mode to the IPv4 over IPv6 manual tunnel.

The configuration in the system view and the configuration in the tunnel interface view are independent of each other.

Example

Set the hop limit of the specified tunnel interface to 100.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol ipv4-ipv6
[Huawei-Tunnel0/0/1] tunnel ipv4-ipv6 hop-limit 100
```

8.12.5 tunnel ipv4-ipv6 traffic-class

Function

The **tunnel ipv4-ipv6 traffic-class** command sets the traffic level of the IPv4 over IPv6 tunnel.

The **undo tunnel ipv4-ipv6 traffic-class** command restores the traffic level to the default value.

By default, the traffic level of the IPv4 over IPv6 tunnel is 0.

Copyright © Huawei Technologies Co., Ltd.

Format

tunnel ipv4-ipv6 traffic-class { **original** | *class-value* }

undo tunnel ipv4-ipv6 traffic-class

Parameters

Parameter	Description	Value
original	Indicates that the value of the Traffic Class field in the IPv6 field of the IPv6 tunnel header uses the value in Traffic Class field of the original packet. The parameter is unavailable now.	-
class-value	Specifies the traffic level of the IPv4 over IPv6 tunnel.	The value is an integer that ranges from 0 to 255.

Views

Tunnel interface view, system view

Default Level

2: Configuration level

Usage Guidelines

The traffic level of the IPv6 tunnel packets refers to the value of the traffic class field in the tunnel packet header of the ingress on the tunnel.

- If this command is configured in the tunnel interface view, it takes effect only on the current tunnel interface.
- If this command is configured in the system view, it takes effect only on the mobile IPv6 network.

Before running the **tunnel ipv4-ipv6 traffic-class** command in the tunnel interface view, run the **tunnel-protocol ipv4-ipv6** command in the same view to set the tunnel mode to the IPv4 over IPv6 manual tunnel.

The configuration in the system view and the configuration in the tunnel interface view are independent of each other.

Example

Set the traffic level of the IPv4 over IPv6 tunnel to 10.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol ipv4-ipv6
[Huawei-Tunnel0/0/1] tunnel ipv4-ipv6 traffic-class 10
```

 Copyright © Huawei Technologies Co., Ltd.