# 6 IP Service Commands



## 6.1 IPv4 Configuration Commands

### 6.1.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

# 6.1.2 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, the IP address 192.168.1.253 255.255.255.0 is configured on VLANIF1 of the S1720GW-E and S1720GWR-E. On other switches, no IP address is configured for an interface.

## Format

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

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

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *ip-address* | Specifies the IP address of an interface. | The value is in dotted decimal notation. |
| *mask* | Specifies a subnet mask. | The value is in dotted decimal notation. |
| *mask-length* | Specifies the mask length. | The value is an integer that ranges from 0 to 32. |
| **sub** | Configures a secondary IP address for an interface. This parameter is optional. To implement communication between multiple subnets of an interface, configure secondary IP addresses for the interface. | - |

## Views

Interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

The **ip address** command configures IP addresses for interfaces on the switch so that the switch 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 following conditions are prohibited for different interfaces on the same switch:

- 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 10.1.2.1/28 and its broadcast address is 10.1.2.15 and the IP address of interface B is 10.1.2.15/26, the configuration fails.

When you run the **undo ip address** command:

- 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**

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 addresses for a Layer 3 interface on the switch, 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.

The subnet IP address cannot be used as the IP address on an interface.

On the S1720GW-E and S1720GWR-E, if no IP address is configured, VLANIF1 uses the IP address 192.168.1.253 255.255.255.0 by default. After VLANIF1 obtains an IP address through DHCP successfully, the IP address 192.168.1.253 255.255.255.0 is deleted.

NOTE

- Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support Ethernet sub-interfaces.
- Only hybrid and trunk interfaces on the preceding switches support Layer 2 Ethernet sub-interface configuration.
- After you run the **undo portswitch** command to switch Layer 2 interfaces on the preceding series of switches into Layer 3 interfaces, you can configure Layer 3 Ethernet sub-interfaces on the interfaces.
- After an interface is added to an Eth-Trunk, sub-interfaces cannot be configured on the interface.
- VLAN termination sub-interfaces cannot be created on a VCMP client.

## Example

# Configure a primary IP address 10.1.0.1 and a secondary IP address 10.2.0.1 for VLANIF10, with subnet mask 255.255.255.0.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ip address 10.1.0.1 255.255.255.0
[HUAWEI-Vlanif10] ip address 10.2.0.1 255.255.255.0 sub
```

# Configure a primary IP address 10.1.0.1 and a secondary IP address 10.2.0.1 for GE0/0/1, with subnet mask 255.255.255.0.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.1.0.1 255.255.255.0
[HUAWEI-GigabitEthernet0/0/1] ip address 10.2.0.1 255.255.255.0 sub
```

# 6.1.3 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* [ **all-address** ]

**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.<br>• *interface-type* specifies the interface type.<br>• *interface-number* specifies the interface number. | - |
| **all-address** | Enables an interface to borrow all IP addresses of another interface. This parameter can be configured only in the VLANIF interface view. | - |

## Views

GE interface view, GE sub-interface view, XGE interface view, XGE sub-interface view, 25GE interface view, 25GE sub-interface view, 40GE interface view, 40GE sub-interface view, 100GE interface view, 100GE sub-interface view, MultiGE interface view, MultiGE sub-interface view, VLANIF interface view, tunnel interface view

## Default Level

2: Configuration level

## Usage Guidelines

An IP unnumbered interface can be a VLANIF interface , an Ethernet interface, an Ethernet sub-interface, or a Tunnel interface.

- An Ethernet interface and an Ethernet sub-interface can only borrow the IP address of a loopback interface. If one end is configured with IP address unnumbered and the other end is configured with an IP address in non-borrow mode, inter-network segment ARP learning must be enabled on both ends.
- A VLANIF interface can only borrow the IP address of a loopback interface. You can set **all-address** to configure a VLANIF interface to borrow all the IP addresses of a loopback interface.
- A Tunnel interface can borrow the IP address of an Ethernet interface, a loopback interface, an Eth-Trunk interface, a VLANIF interface, or a Tunnel interface.

The interface from which the IP address is borrowed must be a Layer 3 interface.

If the interface assigned to an IP unnumbered interface has no IP address, the IP unnumbered interface obtains the IP address 0.0.0.0.

The **ip address unnumbered** command only configures an interface to borrow the IP address from another interface. Other attributes of the interface that borrows an IP address, such as the enablement of routing protocols, need to be configured separately.

## Example

# Configure Tunnel1 to borrow the IP address from LoopBack0.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] ip address unnumbered interface loopback 0
```

# Configure VLANIF 10 to borrow the IP address from LoopBack1.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ip address unnumbered interface loopback 1
```

# 6.1.4 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* ]

**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. | - |

| Parameter | Description | Value |
| --- | --- | --- |
| **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.<br>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.
- Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support sub-interfaces.

## Example

# Display IP information about VLANIF15.

```
<HUAWEI> display ip interface vlanif 15
Vlanif15 current state : UP
Line protocol current state : UP
The Maximum Transmit Unit : 1500 bytes
input packets : 766390, bytes : 41540847, multicasts : 681817
```

```
output packets : 242239, bytes : 14679482, multicasts : 172333
Directed-broadcast packets:
 received packets:            0, sent packets:           0
 forwarded packets:           0, dropped packets:        0
Internet Address is 10.1.1.119/24
Broadcast address : 10.1.1.255
TTL being 1 packet number:    164035
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 6-1** Description of the **display ip interface** command output

| Item | Description |
| --- | --- |
| Vlanif15 current state | Physical status of the interface:<br>• UP: indicates that the interface is physically Up.<br>• DOWN: indicates that the interface is physically Down.<br>• Administratively down: indicates that the administrator has run the **shutdown (interface view)** command on the interface. |
| Line protocol current state | Link layer protocol status of the interface:<br>• UP: The link layer protocol of the interface is running properly.<br>• DOWN: The link layer protocol of the interface is Down or no IP address is configured on the interface. |
| The Maximum Transmit Unit | MTU of the interface. The default MTU of an Ethernet interface or a serial 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 : 766390, bytes : 41540847, multicasts : 681817 | Total number of packets, bytes, and multicast packets received by the interface. |

| Item | Description |
| --- | --- |
| output packets : 242239, bytes : 14679482, multicasts : 172333 | 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. |
| Internet Address is | IP address assigned to the interface and mask length. |
| Broadcast address | Broadcast address of the 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. |
| 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 VLANIF15.

```
<HUAWEI> display ip interface brief vlanif 15
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
Interface                   IP Address/Mask      Physical   Protocol
Vlanif15                    10.1.1.119/24        up         up
```

**Table 6-2** 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 | ^down: indicates that the interface is a backup interface. |
| (l): loopback | The letter "l" refers to loopback. |
| (s): spoofing | The letter "s" refers to spoofing. |
| (E): E-Trunk down | Indicates that the Eth-Trunk is Down because of the protocol negotiation on the E-Trunk. |
| Interface | Interface type and number. |
| IP Address/Mask | IP address and mask of an interface. |
| Physical | Physical status of an interface:<br>• Up: indicates that the interface is physically Up. (l) indicates that the loopback function is configured on the interface.<br>• Down: indicates that the interface becomes faulty.<br>• *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.<br>• !down: indicates that the FIB module is suspended. In this case, the link protocol status of the interface is Down. |

| Item | Description |
| --- | --- |
| Protocol | Link protocol status of the interface:<br>• 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.<br>• Down: indicates that the link protocol of the interface fails or no IP address is configured on the interface.<br>(l) indicates that the loopback function is configured on the interface. |

# 6.2 ARP Configuration Commands

## 6.2.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

## 6.2.2 arp auto-scan enable

### Function

The **arp auto-scan enable** command enables automatic ARP scanning on a sub-interface.

The **undo arp auto-scan enable** command disables automatic ARP scanning on a sub-interface.

By default, automatic ARP scanning is disabled on a sub-interface.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

### Format

**arp auto-scan enable**

**undo arp auto-scan enable**

### Parameters

None

## Views

GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VE sub-interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

After automatic ARP scanning is enabled on a sub-interface of which the IP address mask is greater than or equal to 24 bits and the protocol status is Up, the switch scans IP addresses on the network segment where the sub-interface's primary IP address belongs and learns ARP entries of the remote device immediately.

**Precautions**

Automatic ARP scanning can be enabled on a maximum of 512 sub-interfaces of a switch simultaneously. If automatic ARP scanning is enabled on multiple interfaces simultaneously and the protocol status of the sub-interfaces are Up, the switch sends detection packets to the sub-interfaces, causing a high CPU usage.

To prevent the delay of the interface Up event caused by loop detection, the switch enabled with automatic ARP scanning sends detection packets after a delay of 10s.

When both the interface and protocol status are Up, automatic ARP scanning is performed only once, instead of being performed periodically.

## Example

# Enable automatic ARP scanning.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1.10
[HUAWEI-GigabitEthernet0/0/1.10] arp auto-scan enable
```

# 6.2.3 arp broadcast disable (VLANIF interface view)

## Function

The **arp broadcast disable** command disables a VLANIF interface from broadcasting ARP packets.

The **undo arp broadcast disable** command enables a VLANIF interface to broadcast ARP packets.

By default, VLANIF interfaces are enabled to broadcast ARP packets.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

## Format

**arp broadcast disable**

**undo arp broadcast disable**

## Parameters

None

## Views

VLANIF interface view

## Default Level

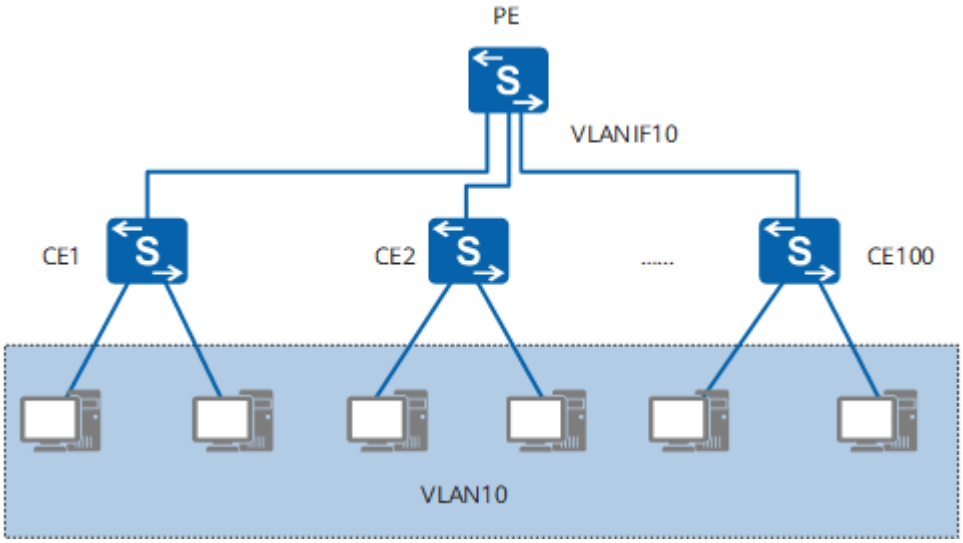
2: Configuration level

## Usage Guidelines

### Usage Scenario

By default, a VLANIF interface broadcasts ARP packets in a VLAN. For example, on the large Layer 2 aggregation network shown in **Figure 6-1**, user hosts connect to CE1 through CE100 to access the aggregation device PE that has VLANIF10 configured as the user gateway. As VLANIF10 by default broadcasts ARP packets, these ARP packets are flooded on the user network, consuming a large number of network resources, which affects services and gateway performance.

**Figure 6-1** Layer 2 aggregation network



To ensure user services and aggregation gateway performance, run the **arp broadcast disable** command to disable the aggregation gateway's VLANIF interface from broadcasting ARP packets.

**Precautions**

Exercise caution when disabling a VLANIF interface from broadcasting ARP packets because this affects the following scenarios in the following ways:

- Proxy ARP scenarios, including intra-VLAN proxy ARP and inter-VLAN proxy ARP

  After a VLANIF interface is disabled from broadcasting ARP packets, the proxy does not forward ARP Request messages from a host to their destinations even if all proxy conditions are met. As a result, proxy ARP fails.

- Scenarios in which hosts send unicast packets

  For example, in ping operations, ICMP Echo Request messages must be encapsulated with MAC addresses mapped to the destination IP addresses. If the host does not have ARP entries, it must send ARP Request messages to learn the MAC address mapped to the destination IP address. However, the VLANIF interface is disabled from broadcasting ARP packets, and therefore cannot send ARP Request messages. Subsequently, the host cannot obtain the MAC address mapped to the destination IP address, causing a ping operation failure. This problem also occurs in other scenarios in which hosts send unicast packets.

- Strict ARP learning scenarios

  In a strict ARP learning scenario, a device learns MAC addresses only of ARP Reply messages in response to ARP Request messages that it sends. If the VLANIF interface is disabled from broadcasting ARP packets, it cannot actively send ARP Request messages. As a result, strict ARP learning fails.

- VLAN aggregation scenarios

  If the VLANIF interface is disabled from broadcasting ARP packets, the super VLAN will not broadcast ARP packets to all its sub-VLANs.

After a VLANIF interface is disabled from broadcasting ARP packets, gratuitous ARP packets will still be sent normally.

Switching between enabling and disabling the ARP broadcasting function on a VLANIF interface will cause the direct routes to flap temporarily.

## Example

# Disable VLANIF 10 from broadcasting ARP packets.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] arp broadcast disable
Warning: This operation will cause the device to fail to send ARP broadcast packets, continue?[Y/N]:y
```

# 6.2.4 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 ARP aging probe mode on an interface.

By default, an interface broadcasts only the last ARP aging probe packet, and unicasts other ARP aging probe packets.

## Format

**arp detect-mode unicast**

**undo arp detect-mode unicast**

## Parameters

None

## Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, VLANIF interface view, VBDIF interface view, VE interface view, port group view

## Default Level

2: Configuration level

## Usage Guidelines

### Usage Scenario

After the aging time of a dynamic ARP entry on an interface expires, the switch sends an aging probe packet (ARP Request packet, and the detection interval is 5 seconds.) from the interface. If the switch receives an ARP Reply packet, it updates this dynamic ARP entry and the aging probe ends. If the switch does not receive an ARP Reply packet after the configured aging probe attempts, it deletes the dynamic ARP entry and the aging probe ends. The aging probe packet can be a unicast or broadcast packet.

If a non-Huawei device receives an ARP aging probe packet with the destination MAC address as the broadcast address from a switch, but the ARP entry of the switch already exists in its ARP table, the non-Huawei device discards the ARP aging probe packet. Failing to receive an ARP Reply to the ARP aging probe packet, the switch deletes the corresponding ARP entry. As a result, the traffic from the network side is interrupted. To resolve this problem, the switch must be configured to send ARP aging probe packets in unicast mode, and the non-Huawei device must be configured to respond to unicast ARP aging probe packets.

### Precautions

If the IP address of the peer device remains the same but the MAC address changes frequently, configuring an interface to send ARP aging probe packets in broadcast mode is recommended.

If the MAC address of the peer device remains the same, the network bandwidth is insufficient, and the aging time of ARP entries is set to a small value,

configuring an interface to send ARP aging probe packets in unicast mode is recommended.

## Example

# Configure the interface VLANIF 100 to unicast ARP aging probe packets.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] arp detect-mode unicast
```

# 6.2.5 arp detect-times

## Function

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

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

The default number of aging probes for dynamic ARP entries is 3.

## Format

**arp detect-times** *detect-times*

**undo arp detect-times**

## Parameters

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

## Views

System view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, VLANIF interface view, VBDIF interface view, VE interface view, port group view

## Default Level

2: Configuration level

## Usage Guidelines

### Usage Scenario

In case that the mapping relationship between the IP address and the MAC address of the peer device exists in the ARP table of the local device, the local

device will directly send data packets rather than ARP request packets to the peer device because the MAC address of the peer device exists in the ARP entry of the local device. If the peer device fails to work but the local device is not informed of the fault or change, the local device will send data packets to its original destination MAC address. This causes the traffic to be interrupted.

Therefore, to enhance the communication reliability, run the **arp detect-times** command to set the aging probe times of a dynamic ARP entry to update the dynamic ARP entry.

After the aging time of a dynamic ARP entry on an interface expires, the switch sends an aging probe packet (ARP Request packet, and the detection interval is 5 seconds.) from the interface. If the switch receives an ARP Reply packet, it updates this dynamic ARP entry and the aging probe ends. If the switch does not receive an ARP Reply packet after the configured aging probe attempts, it deletes the dynamic ARP entry and the aging probe ends.

**Precautions**

- If the number of aging probes is set to 0, the device directly deletes expired dynamic ARP entries.
- In VM migration scenarios with distributed gateways, you are advised to set the number of aging probes to 0 to reduce packet loss.
- The **arp detect-times** command can be configured globally or on the specified interface. If the command is not configured on the interface, the aging detection times 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 detection times of a dynamic ARP entry will be the one configured on the interface.

## Example

# Set the number of aging probes for dynamic ARP entries on VLANIF 100 to 5.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] arp detect-times 5
```

# 6.2.6 arp direct-route enable

## Function

The **arp direct-route enable** command enables the ARP module to send ARP Vlink direct routes to the route management (RM) module.

The **undo arp direct-route enable** command disables the ARP module from sending ARP Vlink direct routes to the RM module.

By default, the ARP module is disabled from sending ARP Vlink direct routes to the RM module.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

## Format

**arp direct-route enable**

**undo arp direct-route enable**

## Parameters

None

## Views

VLANIF interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, Eth-Trunk sub-interface view, 100GE sub-interface view, VE sub-interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

ARP Vlink direct routes are 32-bit host routes that are generated based on ARP entries statically configured or dynamically learned.

In most cases, ARP Vlink direct routes are only used to guide local forwarding. To control the scale and maintain the stability of the routing table, the ARP module does not send ARP Vlink direct routes to the RM module.

In some scenarios, however, the device needs to perform operations based on specific routes of users. For example, the device needs to directly send the network traffic to specific user terminals, or route filtering is used to restrict inter-device communication.

In these scenarios, run the **arp direct-route enable** command to enable the ARP module to send ARP Vlink direct routes to the RM module. This configuration allows the device to select ARP Vlink direct routes based on longest match first to guide traffic forwarding, and accordingly accurately control downstream traffic, which improves the forwarding efficiency.

**Follow-up Procedure**

If you want the device to advertise ARP Vlink direct routes to upstream devices after you enable the ARP module to send ARP Vlink direct routes to the RM module, perform the following operations in sequence:

1. Run the **arp vlink-direct-route advertise** command to configure the device to advertise ARP Vlink direct routes.
2. Configure the device to import the ARP Vlink direct routes to the routing tables of the routing protocols running on the device for the ARP Vlink direct routes to be advertised.

**Precautions**

Currently, the ARP module can only send ARP Vlink direct routes of sub-interfaces and VLANIF interfaces to the RM module.

## Example

# Enable the ARP module to send ARP Vlink direct routes to the RM module.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1.1
[HUAWEI-GigabitEthernet0/0/1.1] arp direct-route enable
```

# 6.2.7 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.

## 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 that ranges from 30 to 62640, in seconds. The default value is 1200 seconds, that is, 20 minutes. |

## Views

System view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, VLANIF interface view, VBDIF interface view, VE interface view, port group view

## Default Level

2: Configuration level

## Usage Guidelines

### Usage Scenario

To ensure communication reliability, you need to update ARP entries when they are invalid. A dynamic ARP entry has a life cycle. If a dynamic ARP entry is not

updated before its life cycle ends, this dynamic ARP entry will be deleted from the ARP table. The life cycle is called aging time. If the entry is updated before its life cycle expires, the aging time of the entry is recalculated.

You can run the **arp expire-time** command to configure the aging time of dynamic ARP entries, ensuring that dynamic ARP entries are updated in time.

After the aging time of a dynamic ARP entry on an interface expires, the switch sends an aging probe packet (ARP Request packet, and the detection interval is 5 seconds.) from the interface. If the switch receives an ARP Reply packet, it updates this dynamic ARP entry and the aging probe ends. If the switch does not receive an ARP Reply packet after the configured aging probe attempts, it deletes the dynamic ARP entry and the aging probe ends.

**Precautions**

- If the aging time set for a dynamic ARP entry is short, the refreshment for the ARP entry will consume huge number of system resources, causing adverse impacts on other services, a network flapping and even traffic forwarding.
- If the aging time set for a dynamic ARP entry is long, the ARP entry will not be promptly updated when it is invalid. For example, if a device fails to work or a network card is changed but the invalid ARP entry has not updated yet, the device sends packets to the peer device based on the existing ARP entry. As a result, the service will be interrupted.

To ensure system stability, use the default value of 20 minutes for a dynamic ARP entry.

If a new aging time is set on an interface that has already learned ARP entries, the new aging time will not take effect on the ARP entries that have been learned, but will take effect on the ARP entries to be learned.

After proxy ARP is enabled on the device, the aging time of ARP entries on user hosts connected to the device should be shortened so that invalid ARP entries on the hosts can be deleted as soon as possible. This decreases packet forwarding failures on the device.

You can adjust the aging parameters of dynamic ARP entries in both the system view and interface view.

- If you configure the parameters only in the system view, the configuration takes effect for the dynamic ARP entries learned on all interfaces of the device.
- If you configure the parameters in both the system and interface views, the configuration in the interface view takes effect only for the dynamic ARP entries learned on the interface specified.
- You cannot adjust the aging parameters of dynamic ARP entries on sub-interfaces. If you configure the parameters on the master interface, the configuration takes effect for the dynamic ARP entries learned on the sub-interfaces. If you do not configure the parameters on the master interface, the configuration in the system view takes effect for the dynamic ARP entries learned on the sub-interfaces.

## Example

# Set the aging time of dynamic ARP entries to 600 seconds on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] arp expire-time 600
```

# 6.2.8 arp fixup

## Function

The **arp fixup** command configures fixed ARP and converts the dynamic ARP entries learned by the device into static ARP entries.

## Format

**arp fixup**

## Parameters

None

## Views

VLANIF interface view, GE interface view, GE sub-interface view, MultiGE interface view, MultiGE sub-interface view, 40GE interface view, 40GE sub-interface view, XGE interface view, 25GE interface view, XGE sub-interface view, 25GE sub-interface view, 100GE interface view, 100GE sub-interface view, Eth-Trunk interface view, or Eth-Trunk sub-interface view

## Default Level

2: Configuration level

## Usage Guidelines

### Usage Scenario

To prevent attackers from forging ARP packets and modifying dynamic ARP entries on the device, you can run the **arp fixup** command on interfaces to configure fixed ARP and convert the dynamic ARP entries learned by the device into static ARP entries.

Fixed ARP is used together with ARP automatic scanning. Run the **arp scan** command to configure ARP automatic scanning so that the device can obtain the dynamic ARP entries from the devices in the network. Then run the **arp fixup** command to configure fixed ARP so that the device converts the obtained dynamic ARP entries to static ARP entries to prevent network attacks.

### Prerequisites

On an Ethernet interface working in Layer 2 mode, the **undo portswitch** command has been run to switch the interface to Layer 3 mode.

**NOTE**

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support switching between Layer 2 and Layer 3 modes.

**Precautions**

- The number of static ARP entries converted through fixed ARP depends on the number of static ARP entries supported on the device. When the number of dynamic ARP entries exceeds the maximum value supported on the device, excess dynamic ARP entries will not be converted and the system displays an error message.
- The static ARP entries converted through fixed ARP are the same as the configured ARP entries. You can run the **undo arp static** command to delete each entry or **reset arp static** to delete all the entries.

## Example

# Configure fixed ARP on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] arp fixup
Warning: This operation may generate configuration of static ARP, and take a long time, press CTRL+C to break. Continue?[Y/N]:y
```

# 6.2.9 arp ip-conflict-detect enable

## Function

The **arp ip-conflict-detect enable** command enables the switch to log IP address conflicts during IP address conflict detection.

The **undo arp ip-conflict-detect enable** command disables the switch from logging IP address conflicts during IP address conflict detection.

By default, IP address conflicts during IP address conflict detection are not logged.

## Format

**arp ip-conflict-detect enable**

**undo arp ip-conflict-detect enable**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

When the IP addresses of devices on the network conflict, the CPU usage becomes excessively high and routes on the devices flap frequently. This greatly affects user services and even results in service interruption. You can run the **arp ip-conflict-detect enable** command to enable the switch to log IP address conflicts during IP address conflict detection. In this way, the device IP addresses can be properly managed, reducing the impact of IP address conflicts on user services.

When a device enabled with IP address conflict detection receives a non-gratuitous ARP packet from a user, the device compares the source IP address and source MAC address of the packet with the ARP entries that the device has learned. If the source IP address matches an ARP entry but the MAC address matches no ARP entry, the IP address conflict occurs. The device then generates log information to inform the user.

**Precautions**

After DAI is configured, the function of disabling the VLANIF interface from sending ARP packets destined for other devices to the CPU is ineffective on the VLANIF interface.

## Example

# Enable the switch to log IP address conflicts during IP address conflict detection.

```
<HUAWEI> system-view
[HUAWEI] arp ip-conflict-detect enable
```

# 6.2.10 arp learning double-tag disable

## Function

The **arp learning double-tag disable** command disables ARP learning for packets with double VLAN tags.

The **undo arp learning double-tag disable** command enables ARP learning for packets with double VLAN tags.

ARP learning is disabled for packets with double VLAN tags.

**NOTE**

Only the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

## Format

**arp learning double-tag disable**

**undo arp learning double-tag disable**

## Parameters

None

## Views

VLANIF interface view

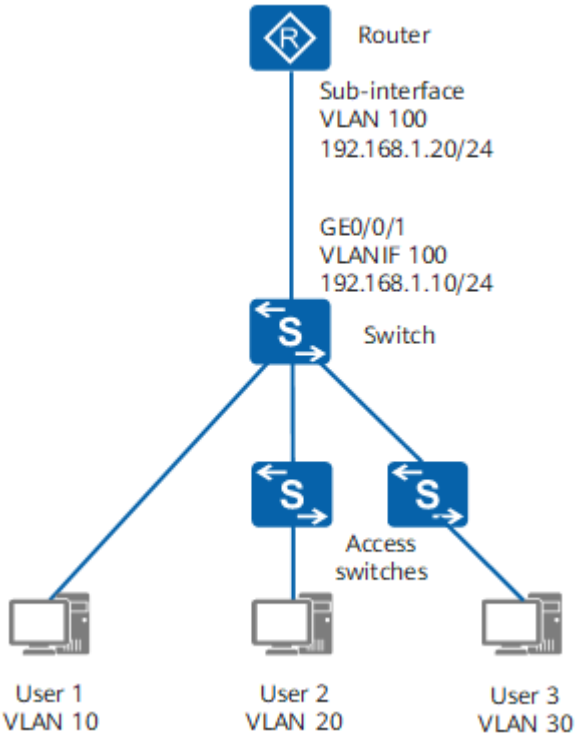
## Default Level

2: Configuration level

## Usage Guidelines

In **Figure 6-2**, users belong to different VLANs and are connected to the gateway router through the switch. The switch is connected to the sub-interface for VLAN termination on the router through VLANIF 100. GE0/0/1 on the switch is configured as a hybrid interface, added to VLAN 10 in untagged mode, and added to VLAN 20 and VLAN 30 in tagged mode. Static ARP binding is configured for user 2 and user 3 on the router, and the inner and outer VLANs are specified.

**Figure 6-2** Networking of disabling ARP learning for packets with double VLAN tags




When the router pings the IP address 192.168.1.10 of VLANIF 100 on the switch, the switch learns an ARP entry containing the IP address 192.168.1.20 and VLAN ID 100 of the router's sub-interface.

When the router sends ARP probe packets to a user (for example, user 2) who is not directly connected to the switch, the source IP address in the probe packets is the IP address 192.168.1.20 of the router's sub-interface, and the probe packets contain double VLAN tags. The outer VLAN ID is 100 and the inner VLAN ID is 20. When the probe packets pass through the switch, the switch updates the original ARP entry, and records the outer VLAN ID 100 and inner VLAN ID 20.

By default, the fast ICMP reply function is enabled on the switch. When receiving ICMP request packets, the receiving interface on the switch does not send the

packets to the CPU for processing, and instead, directly replies with ICMP reply packets. When the router pings the IP address 192.168.1.10 of VLANIF 100 on the switch, ICMP reply packets match the ARP entry containing the IP address 192.168.1.20, and the ARP entry corresponds to the outer VLAN ID 100 and inner VLAN ID 20. Therefore, ICMP reply packets sent by the switch contain double VLAN tags. When checking the VLAN in received packets, the router detects that the packets contain double VLAN tags instead of one VLAN tag, and discards the packets. Therefore, the router fails to ping the IP address 192.168.1.10 of VLANIF 100 on the switch.

You can run the **arp learning double-tag disable** command on the switch to disable ARP learning for packets with double VLAN tags. After this function is disabled, the switch does not learn ARP entries from ARP probe packets with double VLAN tags sent from the router to a user, and does not update the learned ARP entry containing the IP address 192.168.1.20 and VLAN ID 100. The router can always ping the IP address 192.168.1.10 of VLANIF 100 on the switch.

## Example

# Disable ARP learning for packets with double VLAN tags on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] arp learning double-tag disable
```

# 6.2.11 arp learning ip-network-cross enable

## Function

The **arp learning ip-network-cross enable** command enables inter-network segment ARP learning on interfaces.

The **undo arp learning ip-network-cross enable** command disables inter-network segment ARP learning on interfaces.

By default, inter-network segment ARP learning is disabled on interfaces.

## Format

**arp learning ip-network-cross enable**

**undo arp learning ip-network-cross enable**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

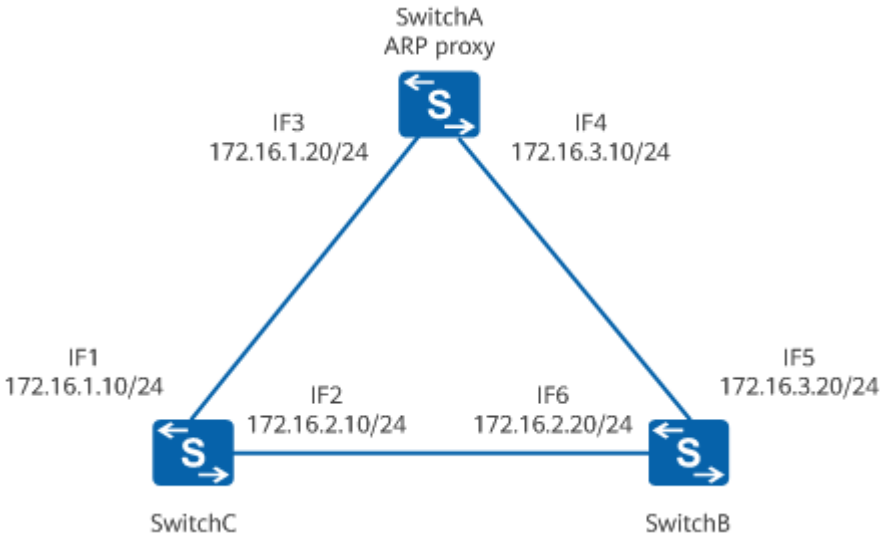
  

## Usage Guidelines

### Usage Scenario

In **Figure 6-3**, a loop prevention protocol has been configured on each switch. SwitchC can learn the ARP entry with the destination IP address 172.16.2.20 (IP address of interface IF6 on SwitchB) through interface IF2. After proxy ARP is enabled on SwitchA, SwitchC can learn ARP entries on another network segment, and interface IF1 on SwitchC can also learn the ARP entry with the destination IP address 172.16.2.20. As a result, the ARP entry learned through interface IF2 is overwritten by that learned through interface IF1, and SwitchC cannot communicate with SwitchB. In this case, you can run the **undo arp learning ip-network-cross enable** command to disable inter-network segment ARP learning on interface IF1 of SwitchC.

**Figure 6-3** Networking for disabling inter-network segment ARP learning




If a switch is upgraded from a version earlier than V200R010C00 to V200R020C00 or a later version, inter-network segment ARP learning is enabled on interfaces by default after the upgrade. In addition, the **undo arp learning ip-network-cross enable** command can be run on such switches, but not the **arp learning ip-network-cross enable** command. If a switch is upgraded from V200R010C00 or a later version to V200R020C00 or a later version, inter-network segment ARP learning is disabled on interfaces by default after the upgrade, and the **arp learning ip-network-cross enable** and **undo arp learning ip-network-cross enable** commands can be run on such switches.

### Precautions

In versions earlier than V200R020C00, this command can be used only for configuration restoration and cannot be manually configured after the configuration is restored.

## Example

# Disable inter-network segment ARP learning on interfaces.

```
<HUAWEI> system-view
[HUAWEI] undo arp learning ip-network-cross enable
```

# 6.2.12 arp learning multicast disable

## Function

The **arp learning multicast disable** command disables an interface from learning ARP entries with multicast MAC addresses.

The **undo arp learning multicast disable** command enables an interface to learn ARP entries with multicast MAC addresses.

By default, if a device is globally enabled to learn ARP entries with multicast MAC addresses, this function is enabled on all the interfaces. If a device is globally disabled from learning ARP entries with multicast MAC addresses, this function is disabled on all the interfaces.

## Format

**arp learning multicast disable**

**undo arp learning multicast disable**

## Parameters

None

## Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, VLANIF interface view, VBDIF interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

An IP address may map a multicast MAC address. In this case, a network administrator has to configure a static ARP entry. After a device is enabled to learn ARP entries with multicast MAC addresses, the device can generate dynamic ARP entries. This reduces a network administrator's workload and decreases network operation and maintenance costs.

After a device is globally enabled to learn ARP entries with multicast MAC addresses, all the interfaces will learn ARP entries when receiving ARP packets with the multicast MAC addresses as source MAC addresses. This increases system resource consumption and affects user service running. You can run the **arp learning multicast disable** command on an interface to disable the interface from learning ARP entries with multicast MAC addresses.

**Precautions**

After an interface is disabled from learning ARP entries with multicast MAC addresses, the interface directly discards ARP packets with the multicast MAC addresses as source MAC addresses, which may result in service interruption.

In the multicast service scenario, if the mapping between IP addresses and multicast MAC addresses is not specified using the **arp static** command, do not disable the specified interface from learning ARP entries with multicast MAC addresses to ensure normal running of the multicast service.

After an interface is disabled from learning ARP entries with multicast MAC addresses using the **arp learning multicast disable** command, you can run the **undo arp learning multicast disable** or **arp learning multicast enable** command on the interface to enable it to learn multicast MAC addresses. The differences between the two commands are as follows:

- After you run the **arp learning multicast enable** command, the configuration on the interface takes effect.
- After you run the **undo arp learning multicast disable** command, the global configuration takes effect.

## Example

# Disable an interface from learning ARP entries with multicast MAC addresses.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp learning multicast disable
```

# 6.2.13 arp learning multicast enable (interface view)

## Function

The **arp learning multicast enable** command enables an interface to learn ARP entries with multicast MAC addresses.

The **undo arp learning multicast enable** command disables an interface from learning ARP entries with multicast MAC addresses.

By default, if a device is globally enabled to learn ARP entries with multicast MAC addresses, this function is enabled on all the interfaces. If a device is globally disabled from learning ARP entries with multicast MAC addresses, this function is disabled on all the interfaces.

## Format

**arp learning multicast enable**

**undo arp learning multicast enable**

## Parameters

None

## Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, MultiGE interface view, Eth-Trunk interface view, VLANIF interface view, VBDIF interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

An IP address may map a multicast MAC address. In this case, a network administrator has to configure a static ARP entry. After a device is enabled to learn ARP entries with multicast MAC addresses, the device can generate dynamic ARP entries. This reduces a network administrator's workload and decreases network operation and maintenance costs.

**Precautions**

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

To prevent the device from being attacked, multicast MAC address learning adopts the most precise matching rule:

- When the function is enabled globally and on an interface, the configuration on the interface takes effect.
- When the function is disabled on an interface, the global configuration takes effect.
- When the function is disabled globally, the configuration on the interface takes effect.

If you run the **undo arp learning multicast enable** command on an interface when the function is enabled globally and on the interface, the global configuration takes effect and the function is still enabled. To completely disable the interface from learning ARP entries with multicast MAC addresses, run the **arp learning multicast disable** command on the interface.

## Example

# Enable GigabitEthernet0/0/1 to learn ARP entries with multicast MAC addresses.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp learning multicast enable
```

# 6.2.14 arp learning multicast enable (system view)

## Function

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

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

By default, a device is globally disabled from learning ARP entries with 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**

An IP address may map a multicast MAC address. In this case, a network administrator has to configure a static ARP entry. After a device is enabled to learn ARP entries with multicast MAC addresses, the device can generate dynamic ARP entries. This reduces a network administrator's workload and decreases network operation and maintenance costs.

**Precautions**

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

The **arp learning multicast enable** and **arp learning multicast disable** commands can be used together on an interface to precisely control the range of ARP entries with multicast MAC addresses to be learned.

## Example

# Globally enable a device to learn ARP entries with multicast MAC addresses.

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

# 6.2.15 arp learning priority high

## Function

The **arp learning priority high** command sets the ARP learning priority of an interface to high.

The **undo arp learning priority high** command sets the ARP learning priority of an interface to low.

By default, the ARP learning priority of an interface is low.

## Format

**arp learning priority high**

**undo arp learning priority high**

## Parameters

None

## Views

VLANIF interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

If the ARP resources of a card are limited, you can configure a high ARP learning priority for VLANIF interfaces that carry important services and reserve certain ARP resources. When the remaining ARP resources of a card are less than or equals the number of reserved ARP entries, only VLANIF interfaces with a high priority can deliver the ARP entries.

- To check the ARP specification based on the value of **HOST4**, run the **display adp-l3 ability** [ **slot** *slot-number* ] command in the diagnostic view.
- To check the number of reserved ARP entries based on the value of **Reserved ARP number**, run the **display adp-ipv4 statistics arp** [ **slot** *slot-id* ] command in the diagnostic view.

**Pre-configuration Tasks**

The **assign arp reserved number** *number-value* command has been run in the system view to configure the number of reserved ARP entries for all cards. The number of reserved ARP entries of each card is displayed as the value of *number-value*.

**Precautions**

If you run the **arp learning priority high** command on multiple VLANIF interfaces of a card, these interfaces share the number of reserved ARP entries of the card.

## Example

# Set the ARP learning priority of VLANIF 10 to high.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
```

```
[HUAWEI-vlan10] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] arp learning priority high
```

# 6.2.16 arp periodic-refresh disable

## Function

The **arp periodic-refresh disable** command disables the function of updating ARP entries every 10 hours.

The **undo arp periodic-refresh disable** command enables the function of updating ARP entries every 10 hours.

By default, the function of updating ARP entries every 10 hours is enabled.

NOTE

For S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: To disable the function of periodically updating ARP entries, run both the **arp periodic-refresh disable** and **undo arp regularly-refresh enable** commands.

## Format

**arp periodic-refresh disable**

**undo arp periodic-refresh disable**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

By default, a device runs a timer to update its ARP entries every 10 hours. To reduce the load on the device, you can run this command to disable the device from updating ARP entries every 10 hours.

## Example

# Disable the device from updating ARP entries every 10 hours.

```
<HUAWEI> system-view
[HUAWEI] arp periodic-refresh disable
```

# 6.2.17 arp purge slowly

## Function

The **arp purge slowly** command enables a device to delete dynamic ARP entries after a delay when a VLANIF member interface goes Down.

The **undo arp purge slowly** command restores the default setting.

By default, a device deletes dynamic ARP entries immediately when a VLANIF member interface goes Down.

## Format

**arp purge slowly**

**undo arp purge slowly**

## Parameters

None

## Views

VLANIF interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

By default, when a VLANIF member interface goes Down, a device immediately deletes the dynamic ARP entries learned by the member interface. At this time, the VLANIF interface needs to relearn ARP entries to forward user traffic. However, in some special networking scenarios, such as the ring or dual-homed networking, a VLANIF member interface going Down does not necessarily mean that its interconnected interface is deleted. The outbound interfaces of ARP entries may change. In this situation, it will take a long time for the device to relearn ARP entries, interrupting user service traffic.

To minimize the preceding impact and accelerate user traffic convergence, run the **arp purge slowly** command to enable the device to delete dynamic ARP entries after a delay when a VLANIF member interface goes Down.

After the **arp purge slowly** command is configured, the device does not immediately delete dynamic ARP entries learned by a VLANIF member interface after it goes Down. Instead, it sends ARP probe packets and then deletes or updates ARP entries depending on whether it receives ARP Reply packets within the ARP aging time:

- If the device does not receive ARP Reply packets, it deletes the dynamic ARP entries.

- If the device receives ARP Reply packets, it updates ARP entries based on information contained in the ARP Reply packets.

**Precautions**

To update ARP entries, a better alternative to ARP aging mechanism is enabling the MAC address-triggered ARP entry update function, because the device learns MAC address entries faster. Therefore, to accelerate user traffic convergence, you are advised to enable ARP entry delayed deletion and the MAC address-triggered ARP entry update function using the **mac-address update arp** command.

The **arp purge slowly** and **arp detect-mode unicast** commands are mutually exclusive on the same VLANIF interface. If they are both run on the same VLANIF interface, the **arp purge slowly** command fails to take effect.

## Example

# Enable a device to delete dynamic ARP entries after a delay when a member interface of VLANIF 100 goes Down.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] arp purge slowly
```

# 6.2.18 arp regularly-refresh cycle-interval

## Function

The **arp regularly-refresh cycle-interval** command sets the interval for updating ARP entries in the device hardware table.

The **undo arp regularly-refresh cycle-interval** command restores the default interval for updating ARP entries in the device hardware table.

By default, the interval for updating ARP entries in the device hardware table is 1 minute.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

## Format

**arp regularly-refresh cycle-interval** *cycle-interval*

**undo arp regularly-refresh cycle-interval**

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *cycle-interval* | Specifies the interval for updating ARP entries in the device hardware table. | The value is an integer in the range from 1 to 1440, in minutes. The default value is 1. |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

After a device learns ARP entries, it saves them to the software table and then delivers them to the hardware table. If the entries in the hardware table are incorrect, packets cannot be forwarded normally. In this case, you can enable the function of periodically updating ARP entries in the device hardware table to correct the ARP entries so that packets can be forwarded normally. You can set the interval for updating ARP entries in the device hardware table as required.

**Precautions**

To reduce the load on a device, when the CPU usage reaches about 50%, the device does not periodically update ARP entries in the device hardware table.

## Example

# Set the interval for updating ARP entries in the device hardware table to 5 minutes.

```
<HUAWEI> system-view
[HUAWEI] arp regularly-refresh cycle-interval 5
```

# 6.2.19 arp regularly-refresh enable

## Function

The **arp regularly-refresh enable** command enables the function of periodically updating ARP entries in the device hardware table.

The **undo arp regularly-refresh enable** command disables the function of periodically updating ARP entries in the device hardware table.

By default, the function of periodically updating ARP entries in the device hardware table is enabled.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

## Format

**arp regularly-refresh enable**

**undo arp regularly-refresh enable**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

After a device learns ARP entries, it saves them to the software table and then delivers them to the hardware table. If the entries in the hardware table are incorrect, packets cannot be forwarded normally. In this case, you can enable the function of periodically updating ARP entries in the device hardware table to correct the ARP entries so that packets can be forwarded normally.

**Precautions**

To reduce the load on a device, when the CPU usage reaches about 50%, the device does not periodically update ARP entries in the device hardware table.

## Example

# Enable the function of periodically updating ARP entries in the device hardware table.

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

# 6.2.20 arp regularly-refresh entry-number

## Function

The **arp regularly-refresh entry-number** command sets the number of ARP entries in the hardware table updated each time.

The **undo arp regularly-refresh entry-number** command restores the default number of ARP entries in the hardware table updated each time.

By default, the number of ARP entries in the hardware table updated each time is 50.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

## Format

**arp regularly-refresh entry-number** *entry-number*

**undo arp regularly-refresh entry-number**

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *entry-number* | Specifies the number of ARP entries in the hardware table updated each time. | The value is an integer in the range from 1 to 100. The default value is 50. |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

After a device learns ARP entries, it saves them to the software table and then delivers them to the hardware table. If the entries in the hardware table are incorrect, packets cannot be forwarded normally. In this case, you can enable the function of periodically updating ARP entries in the device hardware table to correct the ARP entries so that packets can be forwarded normally. You can set the number of ARP entries in the hardware table updated each time as required.

**Precautions**

To reduce the load on a device, when the CPU usage reaches about 50%, the device does not periodically update ARP entries in the device hardware table.

## Example

# Set the number of ARP entries in the hardware table updated each time to 25.

```
<HUAWEI> system-view
[HUAWEI] arp regularly-refresh entry-number 25
```

# 6.2.21 arp regularly-refresh scan-interval

## Function

The **arp regularly-refresh scan-interval** command sets the scan interval for updating ARP entries in the device hardware table.

The **undo arp regularly-refresh scan-interval** command restores the default scan interval for updating ARP entries in the device hardware table.

By default, the scan interval for updating ARP entries in the device hardware table is 1 second.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

## Format

**arp regularly-refresh scan-interval** *scan-interval*

**undo arp regularly-refresh scan-interval**

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *scan-interval* | Specifies the scan interval for updating ARP entries in the device hardware table. | The value is an integer in the range from 1 to 300, in seconds. The default value is 1. |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

### Usage Scenario

After a device learns ARP entries, it saves them to the software table and then delivers them to the hardware table. If the entries in the hardware table are incorrect, packets cannot be forwarded normally. In this case, you can enable the function of periodically updating ARP entries in the device hardware table to correct the ARP entries so that packets can be forwarded normally. You can set the scan interval for updating ARP entries in the device hardware table as required.

### Precautions

To reduce the load on a device, when the CPU usage reaches about 50%, the device does not periodically update ARP entries in the device hardware table.

## Example

# Set the scan interval for updating ARP entries in the device hardware table.

```
<HUAWEI> system-view
[HUAWEI] arp regularly-refresh scan-interval 10
```

# 6.2.22 arp scan

## Function

The **arp scan** command configures ARP automatic scanning. This function enables the device to learn ARP entries by sending ARP Request packets to the network segment of the interface IP address.

## Format

**arp scan** [ *start-ip-address* **to** *end-ip-address* ]

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *start-ip-address* | Specifies the start IP address for ARP automatic scanning.<br>The start IP address must be smaller than or equal to the end IP address. | The value is in dotted decimal notation. |
| *end-ip-address* | Specifies the end IP address for ARP automatic scanning.<br>The end IP address must be greater than or equal to the end IP address. | The value is in dotted decimal notation. |

## Views

VLANIF interface view, GE interface view, GE sub-interface view, MultiGE interface view, MultiGE sub-interface view, 40GE interface view, 40GE sub-interface view, XGE interface view, 25GE interface view, XGE sub-interface view, 25GE sub-interface view, 100GE interface view, 100GE sub-interface view, Eth-Trunk interface view, or Eth-Trunk sub-interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

You can run the **arp scan** command to configure ARP automatic scanning so that the device can quickly learn ARP entries of the neighbors in the same network segment.

ARP automatic scanning is used together with fixed ARP. Run the **arp scan** command to enable the device to obtain dynamic ARP entries from all devices in the network. Then run the **arp fixup** command to configure the device to convert the obtained dynamic ARP entries to static ARP entries to prevent network attacks.

**Prerequisites**

On an Ethernet interface working in Layer 2 mode, the **undo portswitch** command has been run to switch the interface to Layer 3 mode.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support switching between Layer 2 and Layer 3 modes.

**Precautions**

- The start and end IP addresses for ARP automatic scanning must be in the same network segment with the IP address of the interface, and the start IP address must be smaller than or equal to the end IP address.
- If the IP address range is not specified, the device scans only the neighbors within the same network segment as the primary IP address of the interface.
- The device does not scan the IP addresses in ARP entries.
- ARP automatic scanning consumes a large number of system resources. You are advised to perform scanning when the resource usage is low and avoid other operations during scanning.
- A VLAN must be configured on a sub-interface, and only one VLAN can be configured.
- Automatic ARP scanning takes a long time if there is a large number of neighbors within the same network segment as the primary IP address of the interface. You can press **Ctrl+C** to stop scanning. The device generates dynamic ARP entries based on the ARP Reply packets received from neighbors before you stop the scanning. You can run the **display arp dynamic** command in any view to check all the dynamic ARP entries that the device has learned.

## Example

# Enable ARP automatic scanning.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] arp scan
Warning: This operation may take a long time, press CTRL+C to break. Continue?[Y/N]:y
```

# 6.2.23 arp send-packet

## Function

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

## Format

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

NOTE

Only S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **cevid** and *subinterface-number* parameter.

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *ip-address* | Specifies the destination IP address of a unicast ARP Request packet. | The value is in dotted decimal notation. |
| *mac-address* | Specifies the destination MAC address of a unicast ARP Request packet. | The value is in the H-H-H format. An H contains 1 to 4 hexadecimal digits. The value cannot be set to FFFF-FFFF-FFFF. |
| **interface** *interface-type interface-number*[*.subinterface-number* ] | Specifies the outbound interface for a unicast ARP Request packet.<br>• *interface-type* specifies the interface type.<br>• *interface-number* specifies the interface number.<br>• *subinterface-number* specifies the sub-interface number. | - |
| **vid** *vid* | Specifies the outer VLAN tag of a unicast ARP Request packet. | The value is an integer that ranges from 1 to 4094. |
| **cevid** *cevid* | Specifies the inner VLAN tag of a unicast ARP Request packet. | The value is an integer that ranges from 1 to 4094. |

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

The **arp send-packet** command triggers the device to send a unicast ARP Request packet to the user with the specified IP address and MAC address. You can determine whether the peer exists by checking whether the device receives an ARP Reply packet from the peer.

- If the device receives an ARP Reply packet from the peer, the peer exists. The device then generates or updates the ARP entry based on the ARP Reply packet.
- If the device does not receive an ARP Reply packet from the peer, the peer does not exist. The device does not generate an ARP entry in this case.

## Example

# Configure the device to send a unicast ARP Request packet with the destination IP address 10.10.10.1 and destination MAC address 00e0-fc12-3456 from VLANIF 100.

```
<HUAWEI> arp send-packet 10.10.10.1 00e0-fc12-3456 interface vlanif 100
```

# 6.2.24 arp static

## Function

The **arp static** command configures a static ARP entry.

The **undo arp static** command deletes a static ARP entry.

By default, the ARP 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* **interface** *interface-type interface-number*[*.subinterface-number* ]

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

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

**undo arp static** *ip-address mac-address* **interface** *interface-type interface-number*[*.subinterface-number* ]

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

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **cevid** *ce-vid* and *subinterface-number*.

## 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 in a static ARP entry. | The value is in the H-H-H format. An H contains 1 to 4 hexadecimal digits. |
| **vpn-instance** *vpn-instance-name* | Specifies the name of a VPN instance.<br>**NOTE**<br>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 name. |
| **interface** *interface-type interface-number*[*.subinterface-number* ] | Specifies the outbound interface in a static ARP entry.<br>● *interface-type* specifies the interface type.<br>● *interface-number* specifies the interface number.<br>● *subinterface-number* specifies the sub-interface number.<br>**NOTE**<br>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 that ranges from 1 to 4094. |
| **cevid** *ce-vid* | Specifies the inner VLAN ID. | The value is an integer that ranges from 1 to 4094. |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

In most cases, devices on a network can use ARP to dynamically learn ARP entries and age or update the generated dynamic ARP entries. However, when a network encounters an ARP attack, the dynamic ARP entries may be incorrectly updated or aged. As a result, the communication between authorized users becomes abnormal.

Static ARP entries can be neither aged nor overwritten by dynamic ARP entries, ensuring communication security. If a static ARP entry is configured on a device, the device can communicate with the peer device using only the specified MAC address. Network attackers cannot modify the mapping between the IP and MAC addresses using ARP packets, ensuring communication between the two devices. Static ARP entries are generally configured on gateways.

Static ARP entries are applicable when:

- Networks contain critical devices such as servers. In this case, static ARP entries can be configured on the switch. As such, network attackers cannot update the ARP entries containing IP addresses of the critical devices on the switch using ARP attack packets, thereby ensuring communication between users and the critical devices.
- Networks contain user devices with multicast MAC addresses. In this case, static ARP entries can be configured on the switch. In doing so, a device, by default, does not learn ARP entries when the source MAC addresses of received ARP packets are multicast MAC addresses.
- A network administrator wants to prevent an IP address from accessing devices. In this case, static ARP entries can be configured on the switch to bind the IP address to an unavailable MAC address.

An ARP entry includes the IP address, the MAC address, and the outbound interface as well as the outer and inner VLAN tags. The switch can add two VLAN tags to the packets according to the ARP entry during packet forwarding.

**Precautions**

When you configure a static ARP entry, note that:

- When the outbound interface is a Layer 2 Ethernet interface, run the **arp static** *ip-address mac-address* **vid** *vlan-id* [ **cevid** *ce-vid* ] **interface** *interface-type interface-number* [*.subinterface-number* ] command.

  When a static ARP entry is configured for a QinQ termination sub-interface, **vid** specified in this command must be the same as **pe-vid** in the **qinq termination pe-vid ce-vid** command, and **cevid** in this command must be within the value range of **ce-vid** in the **qinq termination pe-vid ce-vid** command.
- When the outbound interface is a Layer 3 Ethernet interface, run the **arp static** *ip-address mac-address* **interface** *interface-type interface-number* command.

- When the VPN instance mapping the ARP entries needs to be specified, run the **arp static** *ip-address mac-address* **vpn-instance** *vpn-instance-name* command.
- When short static ARP entries need to be configured (for example, if the device is connected to an NLB cluster and multi-interface ARP is used), run the **arp static** *ip-address mac-address* command.

The IP address specified by *ip-address* must be in the same network segment as the IP address of the outbound interface specified by **interface** *interface-type interface-number*.

If a new static ARP entry is duplicate with an existing one, the system updates the entry.

You can run the **arp static** command multiple times to configure static ARP entries one by one, or run the **arp scan** and **arp fixup** commands to configure multiple static ARP entries at one time.

## Example

# Configure a static ARP entry that maps the IP address 10.0.0.1 to the MAC address 00e0-fc12-3456.

```
<HUAWEI> system-view
[HUAWEI] arp static 10.0.0.1 00e0-fc12-3456
```

# Configure a static ARP entry that maps the IP address 10.1.1.1 to the MAC address 00e0-fc12-3457. This entry belongs to VLAN 10 and its outbound interface is GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] arp static 10.1.1.1 00e0-fc12-3457 vid 10 interface gigabitethernet 0/0/1
```

# Configure a static ARP entry that maps the IP address 10.1.1.1 to the MAC address 00e0-fc12-3457. This 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 00e0-fc12-3457 vpn-instance vpn1
```

# 6.2.25 arp topology-change disable

## Function

The **arp topology-change disable** command disables the device from responding to TC BPDUs. That is, the device does not age or delete ARP entries when receiving TC BPDUs.

The **undo arp topology-change disable** command enables the device to respond to TC BPDUs.

By default, the device is enabled to respond to TC BPDUs. The device ages or deletes ARP entries when receiving TC BPDUs.

## Format

**arp topology-change disable**

**undo arp topology-change disable**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

When STP detects network topology changes, the device sends TC BPDUs to instruct the ARP module to age or delete ARP entries. The device then needs to relearn ARP entries.

If the network topology changes frequently or there are many ARP entries on the network, ARP entry relearning will cause excess ARP packets to be generated. As a result, a large number of system resources are occupied and services are affected. To address this issue, run the **arp topology-change disable** command to disable the device from responding to TC BPDUs. The device does not age or delete ARP entries even if the network topology changes.

**Precautions**

After the device is disabled from responding to TC BPDUs using the **arp topology-change disable** command, it does not age or delete ARP entries when the network topology changes. If the MAC address-triggered ARP entry update function is not enabled, user services may be interrupted because the device does not update the saved ARP entries in real time. In this case, you are advised to run the **mac-address update arp** command to enable the MAC address-triggered ARP entry update function.

## Example

# Disable the device from aging or deleting ARP entries when the network topology changes.

```
<HUAWEI> system-view
[HUAWEI] arp topology-change disable
```

# 6.2.26 arp-miss message-cache disable

## Function

The **arp-miss message-cache disable** command disables the device from packetizing ARP Miss messages.

The **undo arp-miss message-cache disable** command enables the device to packetize ARP Miss messages.

By default, the device is enabled to packetize ARP Miss messages.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

## Format

**arp-miss message-cache disable**

**undo arp-miss message-cache disable**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

If a host sends an IP packet with an irresolvable destination IP address to the device (there is a routing entry matching the destination IP address but there is no ARP entry matching the next hop of the routing entry), ARP Miss messages are generated on the device. By default, the device packetizes ARP Miss messages and sends them to the CPU, improving the efficiency in processing ARP Miss messages.

When the device is enabled to packetize ARP Miss messages, the device cannot send ICMP Host Unreachable packets or ICMP Redirect packets. To enable these cards to send ICMP Host Unreachable packets and ICMP Redirect packets, run the **arp-miss message-cache disable** command to disable the device from packetizing ARP Miss messages.

## Example

# Disable the device from packetizing ARP Miss messages.

```
<HUAWEI> system-view
[HUAWEI] arp-miss message-cache disable
```

# 6.2.27 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 the hosts not configured with the default gateways are located on the same network segment but different physical networks (different broadcast domains), you can run the **arp-proxy enable** command on the device connected to the hosts to enable routed proxy ARP, implementing IP address resolution between the hosts.

**Precautions**

After DAI is configured, the function of disabling the VLANIF interface from sending ARP packets destined for other devices to the CPU is ineffective on the VLANIF interface.

## Example

# Enable routed proxy ARP on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] arp-proxy enable
```

# Enable routed proxy ARP on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-Gigabitethernet0/0/1] undo portswitch
[HUAWEI-Gigabitethernet0/0/1] arp-proxy enable
```

# 6.2.28 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, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, VE sub-interface view, Eth-Trunk sub-interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

When hosts are located on the same network segment and belong to the same VLAN configured with port isolation, you can run the **arp-proxy inner-sub-vlan-proxy enable** command on the device connected to the hosts to enable intra-VLAN proxy ARP, implementing IP address resolution between the hosts.

**Precautions**

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

After DAI is configured, the function of disabling the VLANIF interface from sending ARP packets destined for other devices to the CPU is ineffective on the VLANIF interface.

## Example

# Enable intra-VLAN proxy ARP on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] arp-proxy inner-sub-vlan-proxy enable
```

# 6.2.29 arp-proxy inter-sub-vlan-proxy enable

## Function

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

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

By default, inter-VLAN proxy ARP is disabled.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support inter-VLAN proxy ARP.

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support sub-interface.

## Format

**arp-proxy inter-sub-vlan-proxy enable**

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

## Parameters

None

## Views

VLANIF interface view, GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view, VE sub-interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

When hosts are located on the same network segment but belong to different VLANs, you can run the **arp-proxy inter-sub-vlan-proxy enable** command on interfaces to enable inter-VLAN proxy ARP, implementing IP address resolution between the hosts.

When hosts are located on the same network segment but belong to different sub-VLANs, you can enable inter-VLAN proxy ARP on the VLANIF interface in a super VLAN.

If inter-VLAN proxy ARP is enabled on a sub-interface, the users on the sub-interface who belong to the same network segment but different VLANs can communicate with each other.

**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.

After inter-VLAN proxy ARP is enabled on a sub-interface or VLANIF interface, whether packets sent by the sub-interface or VLANIF interface carry tags depends on the link type of the corresponding Layer 2 Ethernet interface, regardless of the mode in which the Layer 2 Ethernet interface is added to a VLAN. For example, packets sent from a sub-interface or VLANIF interface on a trunk interface carry VLAN tags.

After DAI is configured, the function of disabling the VLANIF interface from sending ARP packets destined for other devices to the CPU is ineffective on the VLANIF interface.

## Example

# Enable inter-VLAN proxy ARP on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] arp-proxy inter-sub-vlan-proxy enable
```

# 6.2.30 arp-suppress enable

## Function

The **arp-suppress enable** command enables ARP suppression.

The **undo arp-suppress** command disables ARP suppression.

By default, ARP suppression is disabled and applicable only to VLANIF interfaces.

## Format

**arp-suppress enable**

**undo arp-suppress**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

On a special network or in the case of ARP attacks, the system receives multiple ARP packets with the same source IP address at a time. The system needs to update ARP entries repeatedly. To ensure system performance, you can enable ARP suppression. This function enables the system to only respond to ARP Request packets but not update ARP entries when the system receives multiple ARP packets with the same IP address in one second.

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

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

## Example

# Enable ARP suppression.

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

# 6.2.31 assign arp reserved number

## Function

The **assign arp reserved number** command configures the number of reserved ARP entries.

The **undo assign arp reserved number** command cancels the configuration of the number of reserved ARP entries.

By default, the number of reserved ARP entries is 0.

## Format

**assign arp reserved number** *number-value*

**undo assign arp reserved number**

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *number-value* | Specifies the number of reserved ARP entries. | The value is an integer that ranges from 0 to 2000. |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

If the ARP resources of a card are limited, you can set the ARP learning priorities and the number of reserved ARP entries. When the remaining ARP resources of a card are less than or equals the reserved ARP entries, only interfaces with a high priority can deliver ARP entries.

- Run the **display adp-l3 ability** [ **slot** *slot-number* ] command in the diagnostic view to check the ARP specification based on the value of **HOST4**.
- Run the **display adp-ipv4 statistics arp** [ **slot** *slot-id* ] command in the diagnostic view to check the number of reserved ARP entries based on the value of **Reserved ARP number**.

**Follow-up Procedure**

Run the **arp learning priority high** command in the VLANIF interface view to set the ARP learning priority of the VLANIF interface to high.

## Example

# Set the number of reserved ARP entries of each card to 1000.

```
<HUAWEI> system-view
[HUAWEI] assign arp reserved number 1000
```

# 6.2.32 dhcp snooping arp security enable

## Function

The **dhcp snooping arp security enable** command enables the egress ARP inspection (EAI) function.

The **undo dhcp snooping arp security enable** command disables the EAI function.

By default, EAI is disabled.

## Format

**dhcp snooping arp security enable**

**undo dhcp snooping arp security enable**

## Parameters

None

## Views

VLAN view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

EAI applies to the following scenario: A device is deployed between an upstream Layer 3 switch and user hosts. The user hosts belong to the same VLAN, connect to the network through user-side interfaces of the device, and obtain IP addresses through DHCP.

If the device broadcasts ARP Request packets in the VLAN, the traffic volume in the VLAN increases. To reduce network loads in the VLAN, enable EAI in this VLAN on the device. The EAI function must be used together with DHCP snooping.

After EAI is enabled, the device matches the destination IP address of a received ARP Request packet with DHCP snooping binding entries to determine the outbound interface for the packet.

- If the destination IP address matches an entry, the device directly sends the packet to the mapping outbound interface. (However, if the outbound interface is the same as the inbound interface of the packet, the device discards the packet.)
- If the destination IP address does not match an entry, the device determines whether the packet is sent from a trusted interface. (In DHCP snooping, the interfaces connecting the device to the DHCP server are deployed as trusted interfaces.)
  - If the packet is sent from a trusted interface, the device forwards the packet from other trusted interfaces. (If there is no other trusted interface, the device discards the packet.)
  - If the packet is not sent from a trusted interface, the device forwards the packet from a trusted interface.

NOTE

DHCP snooping allows a physical interface to be configured as a trusted or untrusted interface. The interfaces connected to the authorized DHCP server are configured as trusted interfaces, and other interfaces as untrusted interfaces. After DHCP snooping is enabled, all interfaces are considered as untrusted interfaces by default.

**Precautions**

Because the EAI function must be used together with the DHCP snooping function, run the **dhcp snooping enable** command to enable the DHCP snooping function.

After EAI is enabled, the device sends all the received ARP packets to the CPU for software forwarding, which degrades the ARP packet forwarding performance.

The MFF function is implemented based on ARP proxy, whereas the EAI function is implemented based on ARP request packet forwarding. Therefore, the two

functions conflict with each other. If you have enabled both MFF and EAI in the same VLAN, the MFF function takes effect.

EAI enabled in a super VLAN does not take effect.

If a VLANIF interface is created for a VLAN enabled with EAI, EAI does not take effect on the VLAN.

After DAI is configured, the function of disabling the VLANIF interface from sending ARP packets destined for other devices to the CPU is ineffective on the VLANIF interface.

## Example

# Enable EAI.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] dhcp snooping enable
[HUAWEI-vlan100] dhcp snooping arp security enable
```

# 6.2.33 dhcp snooping arp security isolate-forwarding-trust

## Function

The **dhcp snooping arp security isolate-forwarding-trust** command enables the device to forward ARP packets to trusted interfaces when port isolation is enabled on both inbound and outbound interfaces of the device.

The **undo dhcp snooping arp security isolate-forwarding-trust** command disables the device from forwarding packets to trusted interfaces.

By default, the device is disabled from forwarding packets to trusted interfaces when port isolation is enabled on both inbound and outbound interfaces of the device.

## Format

**dhcp snooping arp security isolate-forwarding-trust**

**undo dhcp snooping arp security isolate-forwarding-trust**

## Parameters

None

## Views

VLAN view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

This function applies to the following scenario: A device is deployed between an upstream Layer 3 switch and user hosts. The user hosts belong to the same VLAN, connect to the network through user-side interfaces of the device, and obtain IP addresses through DHCP. Port isolation is configured on the interfaces of the user hosts and intra-VLAN ARP proxy is configured on the Layer 3 switch. This implements Layer 2 isolation and Layer 3 communication between isolated users in the VLAN.

If EAI is also configured on the device, when receiving an ARP Request packet from a user host requesting for another user host, the device matches the destination IP address of the packet with dynamic DHCP snooping binding entries to determine the outbound interface of the packet. If the destination IP address matches an entry, the device directly sends the packet to the destination interface (that is, the interface on the requested user host). If the destination interface is isolated from the inbound interface of the packet, the device discards the packet and the isolated users cannot communicate with each other.

To address this problem, run the **dhcp snooping arp security isolate-forwarding-trust** command. The device then directly forwards the ARP packet to a trusted interface (that is, the interface on the Layer 3 switch). In this case, the intra-VLAN ARP proxy function on the Layer 3 switch allows the isolated users to communicate with each other.

**Prerequisites**

EAI has been enabled using the **dhcp snooping arp security enable** command.

## Example

# Enable the device to forward ARP packets to trusted interfaces in VLAN 100 when port isolation is enabled on both inbound and outbound interfaces of the device.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] dhcp snooping enable
[HUAWEI-vlan100] dhcp snooping arp security enable
[HUAWEI-vlan100] dhcp snooping arp security isolate-forwarding-trust
```

# 6.2.34 display arp

## Function

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

## Format

**display arp** [ **all** ]

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **all** | Displays all ARP entries. | - |

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

You can run this command to check ARP entries mapping a specified IP address. For example, to check ARP entries mapping the IP address 10.1.1.1, run the **display arp all** | **include** *10.1.1.1* command.

## Example

# Display all ARP entries.

```
<HUAWEI> display arp all
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE       INTERFACE   VPN-INSTANCE
                                VLAN/CEVLAN(SIP/DIP)
--------------------------------------------------------------------------------
192.168.50.166  xxxx-xxxx-xxxx            I -         MEth0/0/1
192.168.50.1    xxxx-xxxx-xxx1  20        D-0         MEth0/0/1
192.168.50.165  xxxx-xxxx-xxx2  19        D-0         MEth0/0/1
192.168.50.171  xxxx-xxxx-xxx3  19        D-0         MEth0/0/1
--------------------------------------------------------------------------------
Total:4         Dynamic:3       Static:0     Interface:1
```

**Table 6-3** Description of the **display arp all** command output

| Item | Description |
| --- | --- |
| IP ADDRESS | IP address in the ARP entry. |

| Item | Description |
| --- | --- |
| MAC ADDRESS | MAC address in the ARP entry.<br>**NOTE**<br>If the value of **MAC ADDRESS** is **Incomplete**, the current ARP entry is a temporary one. When IP packets trigger ARP Miss messages, the device generates temporary ARP entries and sends ARP Request packets to the destination network segment.<br>• When a temporary ARP entry is not aged out, before receiving an ARP Reply packet, the device discards the IP packets matching the temporary ARP entry, and no ARP Miss message is triggered.<br>• When a temporary ARP entry is not aged out, after receiving the ARP Reply packet, the device generates a correct ARP entry to replace the temporary entry.<br>• After the temporary ARP entry is aged out, the device deletes this entry.<br>You can run the **arp-fake expire-time** command to adjust the aging time of the temporary ARP entry. |
| EXPIRE(M) | Remaining lifetime of the ARP entry, in minutes.<br>If the remaining lifetime is 0, ARP entry aging probe is to be started. The ARP entry aging time depends on the number of configured aging probe attempts and the number of ARP entries that need to be aged. |

| Item | Description |
| --- | --- |
| TYPE | Entry type and ID of the slot that obtains the entry. The entry type contains 3 bits. The first bit can be any of the following:<br>• I: Interface, indicating the MAC address of the interface<br>• D: Dynamic, indicating a dynamic ARP entry<br>• S: Static, indicating a static ARP entry<br>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 table has been 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.<br>**NOTE**<br>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.<br>The third bit indicates the ID of the slot that obtains the entry. For the ARP entry with the type as I or S, this field displays -. |
| INTERFACE | Type and number of the interface that has learned ARP entries. |
| VPN-INSTANCE | Name of the VPN instance to which the ARP entry belongs.<br>To configure the VPN instance name, run the **ip vpn-instance** command. |

| Item | Description |
| --- | --- |
| VLAN/CEVLAN | ID of the VLAN/CEVLAN to which the ARP entry belongs.<br>**NOTE**<br>Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **CEVLAN** parameter.<br>In a VXLAN network, **SIP** and **DIP** indicate the source and destination IP addresses of a tunnel.<br>**NOTE**<br>Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **SIP/DIP**. |
| Total | Total number of ARP entries. |
| Dynamic | Number of dynamic ARP entries. |
| Static | Number of static ARP entries. |
| Interface | Number of ARP entries for the interface. |

## 6.2.35 display arp dynamic

### Function

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

### Format

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

### Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **vlan** *vlan-id* | Displays the dynamic ARP entries learned in a specified VLAN.<br>If this parameter is not specified, all the dynamic ARP entries learned by the device are displayed. | The value is an integer that ranges from 1 to 4094. |

### Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

You can run the **display arp dynamic** command to check dynamic ARP entries.

## Example

# Display all dynamic ARP entries.

```
<HUAWEI> display arp dynamic
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE INTERFACE      VPN-INSTANCE
                                VLAN/CEVLAN(SIP/DIP)
--------------------------------------------------------------------------------
192.168.50.166  xxxx-xxxx-xxxx            I -  MEth0/0/1
192.168.50.1    xxxx-xxxx-xxx1  13        D-0  MEth0/0/1
192.168.50.165  xxxx-xxxx-xxx2  19        D-0  MEth0/0/1
192.168.50.171  xxxx-xxxx-xxx3  12        D-0  MEth0/0/1
--------------------------------------------------------------------------------
Total:4         Dynamic:3       Static:0     Interface:1
```

**Table 6-4** 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.<br>**NOTE**<br>If the value of **MAC ADDRESS** is **Incomplete**, the current ARP entry is a temporary one. When IP packets trigger ARP Miss messages, the device generates temporary ARP entries and sends ARP Request packets to the destination network segment.<br>• When a temporary ARP entry is not aged out, before receiving an ARP Reply packet, the device discards the IP packets matching the temporary ARP entry, and no ARP Miss message is triggered.<br>• When a temporary ARP entry is not aged out, after receiving the ARP Reply packet, the device generates a correct ARP entry to replace the temporary entry.<br>• After the temporary ARP entry is aged out, the device deletes this entry.<br>You can run the **arp-fake expire-time** command to adjust the aging time of the temporary ARP entry. |

| Item | Description |
| --- | --- |
| EXPIRE(M) | Remaining lifetime of the ARP entry, in minutes.<br>If the remaining lifetime is 0, ARP entry aging probe is to be started. The ARP entry aging time depends on the number of configured aging probe attempts and the number of ARP entries that need to be aged. |

| Item | Description |
| --- | --- |
| TYPE | Entry type and ID of the slot that obtains the entry. The entry type contains 3 bits. The first bit can be any of the following:<br>• I: Interface, indicating the MAC address of the interface<br>• D: Dynamic, indicating a dynamic ARP entry<br>• S: Static, indicating a static ARP entry<br>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 table has been 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.<br>**NOTE**<br>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.<br>The third bit indicates the ID of the slot that obtains the entry. For the ARP entry with the type as I or S, this field displays -. |
| INTERFACE | Type and number of the interface that has learned ARP entries. |
| VPN-INSTANCE | Name of the VPN instance to which the ARP entry belongs.<br>To configure the VPN instance name, run the **ip vpn-instance** command. |

| Item | Description |
| --- | --- |
| VLAN/CEVLAN | ID of the VLAN/CEVLAN to which the ARP entry belongs.<br>**NOTE**<br>Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **CEVLAN** parameter.<br>In a VXLAN network, **SIP** and **DIP** indicate the source and destination IP addresses of a tunnel.<br>**NOTE**<br>Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **SIP/DIP**. |
| Total | Total number of ARP entries. |
| Dynamic | Number of dynamic ARP entries. |
| Static | Number of static ARP entries. |
| Interface | Number of ARP entries for the interface. |

## 6.2.36 display arp error packet

### Function

The **display arp error packet** command displays the last received 10 ARP error packets.

### Format

**display arp error packet**

### Parameters

None

### Views

All views

### Default Level

1: Monitoring level

## Usage Guidelines

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

## Example

# Display the last received 10 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
```

**Table 6-5** Description of the **display arp error packet** command output

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

# 6.2.37 display arp interface

## Function

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

## Format

**display arp interface** *interface-type interface-number*[*.subinterface-number* ]

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *interface-type interface-number*[*.subinterface-number* ] | Specifies the type and number of an interface.<br>• *interface-type* specifies the interface type.<br>• *interface-number* specifies the interface number.<br>• *subinterface-number* specifies the sub-interface number.<br>**NOTE**<br>Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the *subinterface-number* parameter. | - |

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

You can run the **display arp interface** command to view contents of ARP entries when you need to monitor dynamic ARP entries or locate the faults in ARP.

## Example

# Display all ARP entries for VLANIF 10.

```
<HUAWEI> display arp interface Vlanif 10
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE       INTERFACE   VPN-INSTANCE
                                VLAN/CEVLAN(SIP/DIP)
--------------------------------------------------------------------------------
10.1.0.1        xxxx-xxxx-xxxx          I -          Vlanif10
--------------------------------------------------------------------------------
Total:1         Dynamic:0       Static:0     Interface:1
```

**Table 6-6** 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.<br>**NOTE**<br>If the value of **MAC ADDRESS** is **Incomplete**, the current ARP entry is a temporary one. When IP packets trigger ARP Miss messages, the device generates temporary ARP entries and sends ARP Request packets to the destination network segment.<br>• When a temporary ARP entry is not aged out, before receiving an ARP Reply packet, the device discards the IP packets matching the temporary ARP entry, and no ARP Miss message is triggered.<br>• When a temporary ARP entry is not aged out, after receiving the ARP Reply packet, the device generates a correct ARP entry to replace the temporary entry.<br>• After the temporary ARP entry is aged out, the device deletes this entry.<br>You can run the **arp-fake expire-time** command to adjust the aging time of the temporary ARP entry. |
| EXPIRE(M) | Remaining lifetime of the ARP entry, in minutes.<br>If the remaining lifetime is 0, ARP entry aging probe is to be started. The ARP entry aging time depends on the number of configured aging probe attempts and the number of ARP entries that need to be aged. |

| Item | Description |
| --- | --- |
| TYPE | Entry type and ID of the slot that obtains the entry. The entry type contains 3 bits. The first bit can be any of the following:<br>• I: Interface, indicating the MAC address of the interface<br>• D: Dynamic, indicating a dynamic ARP entry<br>• S: Static, indicating a static ARP entry<br>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 table has been 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.<br>**NOTE**<br>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.<br>The third bit indicates the ID of the slot that obtains the entry. For the ARP entry with the type as I or S, this field displays -. |
| INTERFACE | Type and number of the interface that has learned ARP entries. |
| VPN-INSTANCE | Name of the VPN instance to which the ARP entry belongs.<br>To configure the VPN instance name, run the **ip vpn-instance** command. |

| Item | Description |
| --- | --- |
| VLAN/CEVLAN | ID of the VLAN/CEVLAN to which the ARP entry belongs.<br>**NOTE**<br>Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **CEVLAN** parameter.<br>In a VXLAN network, **SIP** and **DIP** indicate the source and destination IP addresses of a tunnel.<br>**NOTE**<br>Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **SIP/DIP**. |
| Total | Total number of ARP entries. |
| Dynamic | Number of dynamic ARP entries. |
| Static | Number of static ARP entries. |
| Interface | Number of ARP entries for the interface. |

# 6.2.38 display arp ip-conflict track

## Function

The **display arp ip-conflict track** command displays records about IP address conflicts detected.

## Format

**display arp ip-conflict track**

## Parameters

None

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

IP address conflicts on a network will result in frequent route flapping on the device and greatly affect user services.

To quickly locate the conflicting IP addresses and better manage device IP addresses, you can run the **display arp ip-conflict track** command to check records about IP address conflicts detected.

## Example

# Display records about IP address conflicts detected.

```
<HUAWEI> display arp ip-conflict track
   Conflict type       : Remote IP conflict
   IP address          : 10.1.1.1
   System time         : 2013-04-07 11:22:29
   Conflict count      : 1
   Suppress count      : 0
   Old interface       : GE0/0/1
   Receive interface   : GE0/0/2
   Old VLAN/CEVLAN     : 100/0
   Receive VLAN/CEVLAN : 100/0
   Old MAC             : 00e0-fc12-3456
   Receive MAC         : 00e0-fc12-3457

   Conflict type       : Local IP conflict
   IP address          : 192.168.10.1
   System time         : 2013-04-07 11:21:10
   Conflict count      : 1
   Suppress count      : 0
   Local interface     : Vlanif10
   Receive interface   : GE0/0/3
   Receive VLAN/CEVLAN : 10/0
   Receive MAC         : 00e0-fc12-3458
```

**Table 6-7** Description of the **display arp ip-conflict track** command output

| Item | Description |
| --- | --- |
| Conflict type | IP address conflict type:<br>• Local IP conflict occurs between a local device and another device.<br>• Remote IP conflict occurs between devices and users attached to a local access device. |
| IP address | Conflicting IP address. |
| System time | System time when an IP address conflict occurs. |
| Conflict count | Number of IP address conflicts.<br>**NOTE**<br>If the ARP entry mapping the IP address is aged or deleted, this field is set to zero. |

| Item | Description |
| --- | --- |
| Suppress count | Number of IP address conflict suppressions.<br>**NOTE**<br>If the ARP entry mapping the IP address is aged or deleted, this field is set to zero. |
| Old interface | Interface recorded in the ARP entry mapping the IP address before a conflict. |
| Local interface | Interface in the ARP entry of the conflicting IP address. |
| Receive interface | Interface that receives ARP packet during a conflict. |
| Old VLAN/CEVLAN | VLAN and CE VLAN recorded in the ARP entry mapping the IP address before a conflict. |
| Receive VLAN/CEVLAN | VLAN and CE VLAN that receive ARP packets during a conflict. |
| Old MAC | MAC address recorded in the ARP entry mapping the IP address before a conflict. |
| Receive MAC | Source MAC address in the ARP packet received during a conflict. |

# 6.2.39 display arp network

## Function

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

## Format

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

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *net-number* | Specifies the network ID. | The value is in dotted decimal notation. |

| Parameter | Description | Value |
| --- | --- | --- |
| *net-mask* | Specifies the subnet mask.<br>If *net-mask* and *mask-length* are not specified, the default mask length is 32. | This value is in dotted decimal notation. |
| *mask-length* | Specifies the mask length.<br>If *net-mask* and *mask-length* are not specified, the default mask length is 32. | The value is an integer that ranges from 1 to 32. |
| **dynamic** | Displays dynamic ARP entries of a specified network segment. | - |
| **static** | Displays static ARP entries of a specified network segment. | - |

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

You can run the **display arp network** command to check ARP entries of a specified network segment.

## 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(SIP/DIP)
--------------------------------------------------------------------------------
10.10.20.9      xxxx-xxxx-xxxx            I -        Vlanif10
10.10.10.6      xxxx-xxxx-xxxx            I -        Vlanif20
--------------------------------------------------------------------------------
Total:2         Dynamic:0       Static:0     Interface:2
```

**Table 6-8** 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.<br>**NOTE**<br>If the value of **MAC ADDRESS** is **Incomplete**, the current ARP entry is a temporary one. When IP packets trigger ARP Miss messages, the device generates temporary ARP entries and sends ARP Request packets to the destination network segment.<br>• When a temporary ARP entry is not aged out, before receiving an ARP Reply packet, the device discards the IP packets matching the temporary ARP entry, and no ARP Miss message is triggered.<br>• When a temporary ARP entry is not aged out, after receiving the ARP Reply packet, the device generates a correct ARP entry to replace the temporary entry.<br>• After the temporary ARP entry is aged out, the device deletes this entry.<br>You can run the **arp-fake expire-time** command to adjust the aging time of the temporary ARP entry. |
| EXPIRE(M) | Remaining lifetime of the ARP entry, in minutes.<br>If the remaining lifetime is 0, ARP entry aging probe is to be started. The ARP entry aging time depends on the number of configured aging probe attempts and the number of ARP entries that need to be aged. |

| Item | Description |
| --- | --- |
| TYPE | Entry type and ID of the slot that obtains the entry. The entry type contains 3 bits. The first bit can be any of the following:<br>• I: Interface, indicating the MAC address of the interface<br>• D: Dynamic, indicating a dynamic ARP entry<br>• S: Static, indicating a static ARP entry<br>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 table has been 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.<br>**NOTE**<br>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.<br>The third bit indicates the ID of the slot that obtains the entry. For the ARP entry with the type as I or S, this field displays -. |
| INTERFACE | Type and number of the interface that has learned ARP entries. |
| VPN-INSTANCE | Name of the VPN instance to which the ARP entry belongs.<br>To configure the VPN instance name, run the **ip vpn-instance** command. |

| Item | Description |
| --- | --- |
| VLAN/CEVLAN | ID of the VLAN/CEVLAN to which the ARP entry belongs.<br>**NOTE**<br>Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **CEVLAN** parameter.<br>In a VXLAN network, **SIP** and **DIP** indicate the source and destination IP addresses of a tunnel.<br>**NOTE**<br>Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **SIP/DIP**. |
| Total | Total number of ARP entries. |
| Dynamic | Number of dynamic ARP entries. |
| Static | Number of static ARP entries. |
| Interface | Number of ARP entries for the interface. |

# 6.2.40 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 view the statistics on ARP packets.

This command displays the ARP packet statistics on the active switch in a stack system.

## Example

# Display the statistics on ARP packets.

```
<HUAWEI> display arp packet statistics
ARP Pkt Received: sum 420066
ARP Received In Message-cache: sum 0
ARP-Miss Msg Received: sum 0
ARP Learnt Count: sum 5
ARP Pkt Discard For Limit: sum 0
ARP Pkt Discard For SpeedLimit: sum 0
ARP Pkt Discard For Proxy Suppress: sum 179578
ARP Pkt Discard For Other: sum 90347
ARP-Miss Msg Discard For SpeedLimit: sum 0
ARP Discard In Message-cache For SpeedLimit: sum 0
ARP-Miss Msg Discard For Other: sum 0
```

**Table 6-9** Description of the display arp packet statistics command output

| Item | Description |
| --- | --- |
| ARP Pkt Received | Number of the received ARP packets. |
| ARP Received In Message-cache | Number of ARP packets received within each second when a switch encapsulates multiple ARP request packets into one packet. |
| ARP-Miss Msg Received | Total number of ARP Miss messages triggered by ARP Miss packets sent to the CPU. |
| ARP Learnt Count | Times of ARP learning. |
| ARP Pkt Discard For Limit | Number of ARP packets discarded due to the ARP entry limit.<br>To configure the maximum number of dynamic ARP entries that an interface can learn, run the **arp-limit** command. |
| 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.<br>To configure a rate limit for ARP packets based on the source IP address, run the **arp speed-limit source-ip** command. |
| 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. |

| Item | Description |
| --- | --- |
| ARP-Miss Msg Discard For SpeedLimit | Number of ARP Miss messages discarded when the number of ARP Miss messages triggered by IP packets from a specified source IP address exceeds the limit. |
| ARP Discard In Message-cache For SpeedLimit | Number of ARP packets discarded due to software rate limit when a switch encapsulates multiple ARP request packets into one packet.<br>To configure a rate limit for ARP Miss messages based on the source IP address, run the **arp-miss speed-limit source-ip** command. |
| ARP-Miss Msg Discard For Other | Number of the ARP Miss messages discarded due to other causes. |

# 6.2.41 display arp static

## Function

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

## Format

**display arp static**

## Parameters

None

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

You can run the **display arp static** command to check static ARP entries.

You can run the **arp static** command multiple times to configure static ARP entries one by one, or run the **arp scan** and **arp fixup** commands to configure multiple static ARP entries at one time.

## Example

# Display all static ARP entries.

```
<HUAWEI> display arp static
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE       INTERFACE   VPN-INSTANCE
                                VLAN/CEVLAN(SIP/DIP)
--------------------------------------------------------------------------------
10.1.2.1        00e0-fc12-3456            S--
--------------------------------------------------------------------------------
Total:1         Dynamic:0       Static:1     Interface:0
```

**Table 6-10** 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.<br>**NOTE**<br>If the value of **MAC ADDRESS** is **Incomplete**, the current ARP entry is a temporary one. When IP packets trigger ARP Miss messages, the device generates temporary ARP entries and sends ARP Request packets to the destination network segment.<br>• When a temporary ARP entry is not aged out, before receiving an ARP Reply packet, the device discards the IP packets matching the temporary ARP entry, and no ARP Miss message is triggered.<br>• When a temporary ARP entry is not aged out, after receiving the ARP Reply packet, the device generates a correct ARP entry to replace the temporary entry.<br>• After the temporary ARP entry is aged out, the device deletes this entry.<br>You can run the **arp-fake expire-time** command to adjust the aging time of the temporary ARP entry. |
| EXPIRE(M) | Remaining lifetime of the ARP entry, in minutes.<br>If the remaining lifetime is 0, ARP entry aging probe is to be started. The ARP entry aging time depends on the number of configured aging probe attempts and the number of ARP entries that need to be aged. |

| Item | Description |
| --- | --- |
| TYPE | Entry type and ID of the slot that obtains the entry. The entry type contains 3 bits. The first bit can be any of the following:<br>• I: Interface, indicating the MAC address of the interface<br>• D: Dynamic, indicating a dynamic ARP entry<br>• S: Static, indicating a static ARP entry<br>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 table has been 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.<br>**NOTE**<br>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.<br>The third bit indicates the ID of the slot that obtains the entry. For the ARP entry with the type as I or S, this field displays -. |
| INTERFACE | Type and number of the interface that has learned ARP entries. |
| VPN-INSTANCE | Name of the VPN instance to which the ARP entry belongs.<br>To configure the VPN instance name, run the **ip vpn-instance** command. |

| Item | Description |
| --- | --- |
| VLAN/CEVLAN | ID of the VLAN/CEVLAN to which the ARP entry belongs.<br>**NOTE**<br>Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **CEVLAN** parameter.<br>In a VXLAN network, **SIP** and **DIP** indicate the source and destination IP addresses of a tunnel.<br>**NOTE**<br>Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **SIP/DIP**. |
| Total | Total number of ARP entries. |
| Dynamic | Number of dynamic ARP entries. |
| Static | Number of static ARP entries. |
| Interface | Number of ARP entries for the interface. |

# 6.2.42 display arp statistics

## Function

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

## Format

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

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **all** | Displays ARP entry statistics of the device. | - |
| **interface** *interface-type interface-number* | Displays ARP entry statistics of a specified interface.<br>• *interface-type* specifies the interface type.<br>• *interface-number* specifies the interface number. | - |

| Parameter | Description | Value |
| --- | --- | --- |
| **slot** *slot-id* | Displays ARP entry statistics of a specified slot. | The value depends on the device configuration. |

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

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

## Example

# Display ARP entry statistics of the device.

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

# Display ARP entry statistics of slot 0.

```
<HUAWEI> display arp statistics slot 0
Capacity: 98304       In-used: 0
```

**Table 6-11** Description of the **display arp statistics** command output

| Item | Description |
| --- | --- |
| Dynamic | Number of dynamic ARP entries. |
| Static | Number of static ARP entries. |
| Capacity | Maximum number of ARP entries of the device.<br>The ARP entry specifications of a device vary according to the device version and model. |
| In-used | Number of current ARP entries on the device. |

# 6.2.43 display arp status

## Function

The **display arp status** command displays the delivery status of ARP entries on a device.

## Format

**display arp status** *ip-address* [ **vpn-instance** *vpn-instance-name* ] **slot** *slot-id*

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *ip-address* | Specifies an IP address. | 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 name. |
| **slot** *slot-id* | Specifies a slot ID. | Set the value according to the device configuration. |

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

You can run the **display arp status** command to check the delivery status of ARP entries with a specified IP address on a device.

## Example

# Display the delivery status of ARP entries on card 0.

```
<HUAWEI> display arp status 10.137.216.1 slot 0
TYPE : D - Dynamic, I - Interface, S - Static
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE       INTERFACE   VPN-
INSTANCE
                                VLAN/CEVLAN                STATE
--------------------------------------------------------------------------------
10.137.216.1    xxxx-xxxx-xxxx  20        D-0        GE0/0/1
                                4094/-                 Available
--------------------------------------------------------------------------------
```

**Table 6-12** Description of the **display arp status** command output

| Item | Description |
| --- | --- |
| IP ADDRESS | IP address in the ARP entry. |

| Item | Description |
| --- | --- |
| MAC ADDRESS | MAC address in the ARP entry.<br>**NOTE**<br>If the value of **MAC ADDRESS** is **Incomplete**, the current ARP entry is a temporary one. When IP packets trigger ARP Miss messages, the device generates temporary ARP entries and sends ARP Request packets to the destination network segment.<br>• When a temporary ARP entry is not aged out, before receiving an ARP Reply packet, the device discards the IP packets matching the temporary ARP entry, and no ARP Miss message is triggered.<br>• When a temporary ARP entry is not aged out, after receiving the ARP Reply packet, the device generates a correct ARP entry to replace the temporary entry.<br>• After the temporary ARP entry is aged out, the device deletes this entry.<br>You can run the **arp-fake expire-time** command to adjust the aging time of the temporary ARP entry. |
| EXPIRE(M) | Remaining lifetime of the ARP entry, in minutes.<br>If the remaining lifetime is 0, ARP entry aging probe is to be started. The ARP entry aging time depends on the number of configured aging probe attempts and the number of ARP entries that need to be aged. |

| Item | Description |
| --- | --- |
| TYPE | Entry type and ID of the slot that obtains the entry. The entry type contains 3 bits. The first bit can be any of the following:<br>• I: Interface, indicating the MAC address of the interface<br>• D: Dynamic, indicating a dynamic ARP entry<br>• S: Static, indicating a static ARP entry<br>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 table has been 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.<br>**NOTE**<br>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.<br>The third bit indicates the ID of the slot that obtains the entry. For the ARP entry with the type as I or S, this field displays -. |
| INTERFACE | Type and number of the interface that has learned ARP entries. |
| VPN-INSTANCE | Name of the VPN instance to which the ARP entry belongs.<br>To configure the VPN instance name, run the **ip vpn-instance** command. |

| Item | Description |
| --- | --- |
| VLAN/CEVLAN | ID of the VLAN/CEVLAN to which the ARP entry belongs.<br>**NOTE**<br>Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **CEVLAN** parameter. |
| STATE | Whether the ARP entry has been delivered to the chip.<br>• Available: The ARP entry has been delivered to the chip.<br>• Unavailable: The ARP entry has not been delivered to the chip. |

# 6.2.44 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 the change time.

**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 learned by the VLANIF interface change to other interfaces.
- No outbound interface is specified in the static ARP entries. The outbound interfaces change to other interfaces.
- Dynamic ARP entries or static ARP entries in which no VLAN ID and outbound interface are 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 learned.
- The VLAN ID and outbound interface are manually specified in static ARP entries.

## Example

# Display changes of outbound interfaces in 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    xxxx-xxxx-xxxx  1000   GE0/0/1    GE0/0/2    2017-08-19 12:10:12
D  10.2.1.100  xxxx-xxxx-xxx1  300               GE0/0/3    2017-08-19 12:12:12
```

**Table 6-13** Description of the **display arp track** command output

| Item | Description |
| --- | --- |
| Op | Operation code.<br>• M: Modify, indicating that the outbound interface changes.<br>• 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. |
| System-Time | System time when the outbound interface changes. |

# 6.2.45 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 name. |
| **dynamic** | Displays dynamic ARP entries. | - |
| **static** | Displays static ARP entries. | - |

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

You can run the **display arp vpn-instance** command to check ARP entries of a specified VPN instance.

## Example

# Check all ARP entries learned by the VPN instance **r1**.

```
<HUAWEI> display arp vpn-instance r1
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE       INTERFACE   VPN-INSTANCE
                                VLAN/CEVLAN(SIP/DIP)
--------------------------------------------------------------------------------
192.168.1.11    00e0-fc12-3456            I -        Vlanif10       r1
192.168.1.1     00e0-fc12-3455  12        D-0        Vlanif10       r1
--------------------------------------------------------------------------------
Total:2         Dynamic:1       Static:0    Interface:1
```

**Table 6-14** 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.<br>**NOTE**<br>If the value of **MAC ADDRESS** is **Incomplete**, the current ARP entry is a temporary one. When IP packets trigger ARP Miss messages, the device generates temporary ARP entries and sends ARP Request packets to the destination network segment.<br>● When a temporary ARP entry is not aged out, before receiving an ARP Reply packet, the device discards the IP packets matching the temporary ARP entry, and no ARP Miss message is triggered.<br>● When a temporary ARP entry is not aged out, after receiving the ARP Reply packet, the device generates a correct ARP entry to replace the temporary entry.<br>● After the temporary ARP entry is aged out, the device deletes this entry.<br>You can run the **arp-fake expire-time** command to adjust the aging time of the temporary ARP entry. |
| EXPIRE(M) | Remaining lifetime of the ARP entry, in minutes.<br>If the remaining lifetime is 0, ARP entry aging probe is to be started. The ARP entry aging time depends on the number of configured aging probe attempts and the number of ARP entries that need to be aged. |

| Item | Description |
| --- | --- |
| TYPE | Entry type and ID of the slot that obtains the entry. The entry type contains 3 bits. The first bit can be any of the following:<br>• I: Interface, indicating the MAC address of the interface<br>• D: Dynamic, indicating a dynamic ARP entry<br>• S: Static, indicating a static ARP entry<br>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 table has been 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.<br>**NOTE**<br>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.<br>The third bit indicates the ID of the slot that obtains the entry. For the ARP entry with the type as I or S, this field displays -. |
| INTERFACE | Type and number of the interface that has learned ARP entries. |
| VPN-INSTANCE | Name of the VPN instance to which the ARP entry belongs.<br>To configure the VPN instance name, run the **ip vpn-instance** command. |

| Item | Description |
| --- | --- |
| VLAN/CEVLAN | ID of the VLAN/CEVLAN to which the ARP entry belongs.<br>**NOTE**<br>Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **CEVLAN** parameter.<br>In a VXLAN network, **SIP** and **DIP** indicate the source and destination IP addresses of a tunnel.<br>**NOTE**<br>Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **SIP/DIP**. |
| Total | Total number of ARP entries. |
| Dynamic | Number of dynamic ARP entries. |
| Static | Number of static ARP entries. |
| Interface | Number of ARP entries for the interface. |

# 6.2.46 display mac-address multiport

## Function

The **display mac-address multiport** command displays MAC address entries configured for multiple outbound interfaces.

## Format

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

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

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

## Parameters

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

| Parameter | Description | Value |
| --- | --- | --- |
| **vlan** *vlan-id* | Specifies a VLAN. | The value is an integer that ranges from 1 to 4094. |
| **total-number** | Specifies the number of MAC address entries mapping multiple outbound interfaces. | - |

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

You can run the **display mac-address multiport** command to check MAC address entries configured for multiple outbound interfaces. If no parameter is specified, all MAC address entries configured for multiple outbound interfaces are displayed. To configure MAC address entries mapping multiple outbound interfaces, run the **mac-address multiport interface** or **mac-address multiport** command.

## Example

# Display MAC address entries configured for multiple outbound interfaces in VLAN 10.

```
<HUAWEI> display mac-address multiport vlan 10
--------------------------------------------------------------------------------
MAC Address       VLANID    Out-Interface               Status
--------------------------------------------------------------------------------
XXXX-XXXX-XXXX    10        GigabitEthernet0/0/1        Active
                                1 port(s)
--------------------------------------------------------------------------------
 Total Group(s) : 1
```

**Table 6-15** Description of the **display mac-address multiport** command output

| Item | Description |
| --- | --- |
| MAC Address | - |
| VLANID | VLAN that the outbound interface mapping the destination MAC address belongs to. |
| Out-Interface | Outbound interface mapping the destination MAC address. |

| Item | Description |
| --- | --- |
| Status | Current VLAN status, including:<br>• InActive: indicates that no VLAN is created or a VLAN is created but no physical interface is added to the VLAN.<br>• Active: indicates that a VLAN has been created and physical interfaces are added to the VLAN. |
| Total Group(s) | Total number of MAC address entries mapping multiple outbound interfaces. |

# 6.2.47 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 executed, all ARP entries mapping the VLAN to which the Layer 2 interface belongs are updated if the Layer 2 interface turns Up.

NOTE

When an active/standby switchover is performed in a stack, all ARP entries mapping the VLAN to which the Layer 2 interface belongs are updated.

### Example

# Enable Layer 2 topology detection.

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

## 6.2.48 mac-address multiport

### Function

The **mac-address multiport** command configures MAC address entries mapping multiple outbound interfaces in the interface view.

The **undo mac-address multiport** command deletes the MAC address entries mapping multiple outbound interfaces in the interface view.

By default, no MAC address entries on the device map multiple outbound interfaces.

### Format

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

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

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

### Parameters

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

### Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

### Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

The servers in an NLB server cluster use the same IP address (cluster IP address) and MAC address (cluster MAC address). When a device functioning as the access gateway connects to the NLB server cluster, the device needs to send the packet destined to the cluster IP address to each server in the cluster. In this case, run the **mac-address multiport** or **mac-address multiport interface** command to configure MAC address entries mapping multiple outbound interfaces, and run the **arp static** command to configure short static ARP entries. By configuring short static ARP entries, you can determine the MAC address and VLAN mapping the cluster IP address. Query the MAC address table based on the MAC address and VLAN to determine multiple outbound interfaces, and then connect the interfaces to the NLB server cluster.

**Precautions**

The VLAN specified in the **mac-address multiport** command cannot be a MAC VLAN, super VLAN, leased line VLAN, or control VLAN of Smart Ethernet Protection (SEP) and Rapid Ring Protection Protocol (RRPP).

On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, when the outbound interfaces are Eth-Trunk interfaces, you must run the **unknown-unicast load-balance enhanced** command to configure enhanced load balancing for unknown unicast packets. Otherwise, the configuration is invalid.

## Example

# Configure entries of the destination MAC address XXXX-XXXX-XXXX mapping multiple outbound interfaces in VLAN 100 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mac-address multiport XXXX-XXXX-XXXX vlan 100
```

# Configure entries of the destination MAC address XXXX-XXXX-XXXX mapping multiple outbound interfaces in VLAN 100 on Eth-Trunk 6.

```
<HUAWEI> system-view
[HUAWEI] unknown-unicast load-balance enhanced
[HUAWEI] interface eth-trunk 6
[HUAWEI-Eth-Trunk6] mac-address multiport XXXX-XXXX-XXXX vlan 100
```

# 6.2.49 mac-address multiport interface

## Function

The **mac-address multiport interface** command configures MAC address entries mapping multiple outbound interfaces in the system view.

The **undo mac-address multiport interface** command deletes the MAC address entries mapping multiple outbound interfaces in the system view.

By default, no MAC address entries on the device map multiple outbound interfaces.

## Format

**mac-address multiport** *mac-address* **interface** { *interface-type interface-number1* [ **to** *interface-type interface-number2* ] } &<1-10> **vlan** *vlan-id*

**undo mac-address multiport** *mac-address* **interface** { *interface-type interface-number1* [ **to** *interface-type interface-number2* ] } &<1-10> **vlan** *vlan-id*

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

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *mac-address* | Specifies a MAC address. | The value is in the H-H-H format. An H contains 1 to 4 hexadecimal digits. |
| *interface-type interface-number1* [ **to** *interface-type interface-number2* ] | Specifies the interface type and number.<br>• *interface-type* specifies the interface type.<br>• *interface-number1* specifies the first interface number mapping a MAC address entry.<br>• *interface-number2* specifies the last interface number mapping a MAC address entry. The value of *interface-number2* must be greater than that of *interface-number1*, and *interface-number1* and *interface-number2* determine an interface range. | - |
| **vlan** *vlan-id* | Specifies a VLAN that interfaces belong to. | The value is an integer that ranges from 1 to 4094. |
| **all** | Specifies all MAC address entries mapping multiple outbound interfaces. | - |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

The servers in an NLB server cluster use the same IP address (cluster IP address) and MAC address (cluster MAC address). When a device functioning as the access gateway connects to the NLB server cluster, the device needs to send the packet destined to the cluster IP address to each server in the cluster. In this case, run the **mac-address multiport interface** or **mac-address multiport** command to configure MAC address entries mapping multiple outbound interfaces, and run the **arp static** command to configure short static ARP entries. By configuring short static ARP entries, you can determine the MAC address and VLAN mapping the cluster IP address. Query the MAC address table based on the MAC address and VLAN to determine multiple outbound interfaces, and then connect the interfaces to the NLB server cluster.

**Precautions**

The VLAN specified in the **mac-address multiport interface** command cannot be a MAC VLAN, super VLAN, leased line VLAN, or control VLAN of Smart Ethernet Protection (SEP) and Rapid Ring Protection Protocol (RRPP).

On the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S, when the outbound interfaces are Eth-Trunk interfaces, you must run the **load-balance** command to configure load balancing based on IP addresses. Otherwise, the configuration is invalid.

## Example

# Configure entries of the destination MAC address 00e0-fc00-2200 mapping the outbound interfaces GE0/0/1-GE0/0/4 in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] mac-address multiport 00e0-fc00-2200 interface gigabitethernet 0/0/1 to gigabitethernet 0/0/4 vlan 100
```

# Configure entries of the destination MAC address 00e0-fc00-2200 mapping the outbound interfaces Eth-Trunk 4-Eth-Trunk 6 in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] unknown-unicast load-balance enhanced
[HUAWEI] mac-address multiport 00e0-fc00-2200 interface eth-trunk 4 to eth-trunk 6 vlan 10
```

# 6.2.50 reset arp

## Function

The **reset arp** command clears ARP entries and related packet statistics.

## Format

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

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **dynamic** | Clears dynamic ARP entries | - |
| **interface** *interface-type interface-number*[*.subinterface-number* ] | Specifies the interface type and number.<br>• *interface-type* specifies the type of the interface.<br>• *interface-number*[*.subinterface-number* ] specifies the number of the interface or sub interface. | - |
| **ip** *ip-address* | Clears dynamic ARP entries with a specified IP address. | The value is in dotted decimal notation. |
| **vpn-instance** *vpn-instance-name* | Specifies the VPN instance name. | The value must be an existing VPN instance name. |
| **static** | 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 an attacked device learns a large number of invalid ARP entries, ARP entries of valid users may fail to be saved and these users may fail to access the network. The **reset arp** command can be used to delete ARP entries. After that, the device relearns ARP entries to ensure that users can access the network.

To delete ARP entries based on a certain IP address, you can run the **reset arp dynamic ip** *ip-address* [ **vpn-instance** *vpn-instance-name* ] or **reset arp interface** *interface-type interface-number*[*.subinterface-number* ] **ip** *ip-address* command.

**Precautions**

- The **reset arp** command deletes mappings between IP addresses and MAC addresses. As a result, users may fail to access some network devices and services may be interrupted.
- The minimum interval for running the command (only the **reset arp** command in which **ip** *ip-address* is not specified) to clear ARP entries is 20 seconds.

## Example

# Clear dynamic ARP entries.

```
<HUAWEI> reset arp dynamic
```

# Clear dynamic ARP entries of VLANIF 100.

```
<HUAWEI> reset arp interface vlanif 100
```

# Clear the dynamic ARP entry corresponding to the IP address of 10.1.1.1 in VPN 1.

```
<HUAWEI> reset arp dynamic ip 10.1.1.1 vpn-instance vpn1
```

# 6.2.51 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

2: Configuration 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 on the active switch in a stack system.

### Example

# Clear the statistics on all ARP packets.

```
<HUAWEI> reset arp packet statistics
```

# 6.3 DHCP Configuration Commands

## 6.3.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

Layer 3 ethernet interface, VLANIF interface, and sub-interface all support the DHCP function.

## 6.3.2 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**.<br>**NOTE**<br>The percentage of the clear alarms cannot exceed that of the alarms. |

| Parameter | Description | Value |
| --- | --- | --- |
| *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.

**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
```

# 6.3.3 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. When double 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

### 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 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
```

# 6.3.4 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**

## 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 **ip pool** 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
```

# 6.3.5 dhcp anti-attack check duplicate option

## Function

The **dhcp anti-attack check duplicate option** command enables the device to check and discard DHCP messages with duplicate options.

The **undo dhcp anti-attack check duplicate option** command disables the device from checking and discarding DHCP messages with duplicate options.

By default, the device is disabled from checking and discarding DHCP messages with duplicate options.

## Format

**dhcp anti-attack check duplicate option** [ *option-start* [ **to** *option-end* ] ] &<1-254>

**undo dhcp anti-attack check duplicate option** [ *option-start* [ **to** *option-end* ] ] &<1-254>

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *option-start* [ **to** *option-end* ] | Specifies the option value.<br>• *option-start*: Specifies the start value of an option in a DHCP packet.<br>• *option-end*: Specifies the end value of an option in a DHCP packet. | The value is an integer in the range 1 to 254. For an option, the end value must be larger than the start value. |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

The **dhcp anti-attack check duplicate option** command applies to DHCP servers, DHCP relay agents, DHCP clients, and DHCP snooping-enabled devices. To discard DHCP messages with duplicate options 1 to 254, run the **dhcp anti-attack check duplicate option** command.

**Prerequisites**

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

## Example

# Configure the device to discard DHCP messages with duplicate options.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp anti-attack check duplicate option
```

# 6.3.6 dhcp anti-attack check udp-checksum

## Function

The **dhcp anti-attack check udp-checksum** command enables the function of checking the UDP header checksum in a DHCP packet and discarding a DHCP packet with an incorrect checksum.

The **undo dhcp anti-attack check udp-checksum** command disables the function of checking the UDP header checksum in a DHCP packet.

By default, a device checks the UDP header checksum in a DHCP packet and discards a DHCP packet with an incorrect checksum.

## Format

**dhcp anti-attack check udp-checksum**

**undo dhcp anti-attack check udp-checksum**

## Parameters

None

## Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

The **dhcp anti-attack check udp-checksum** command applies to DHCP servers, DHCP relay agents, DHCP clients, and DHCP snooping-enabled devices. Devices from different vendors may use different DHCP implementation mechanisms. After checking the UDP header checksum in a received DHCP packet, a device may not allow the DHCP packet to pass through and discards the packet. As a result, DHCP becomes unavailable. To solve this problem, you can run the **undo dhcp anti-attack check udp-checksum** command to disable the function of checking the UDP header checksum in a DHCP packet, so that a DHCP packet with an incorrect UDP header checksum can be properly forwarded.

**Prerequisites**

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

## Example

# Disable the function of checking the UDP header checksum in a DHCP packet.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] undo dhcp anti-attack check udp-checksum
```

# 6.3.7 dhcp anti-attack check magic-cookie

## Function

The **dhcp anti-attack check magic-cookie** command enables the function of checking the magic-cookie field in a DHCP packet and discarding a DHCP packet with an incorrect value in the magic-cookie field.

The **undo dhcp anti-attack check magic-cookie** command disables the function of checking the magic-cookie field in a DHCP packet.

By default, a device does not check the magic-cookie field in a DHCP packet but directly forwards a DHCP packet with an incorrect value in the magic-cookie field.

## Format

**dhcp anti-attack check magic-cookie**

**undo dhcp anti-attack check magic-cookie**

## Parameters

None

## Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

The **dhcp anti-attack check magic-cookie** command applies to DHCP servers, DHCP relay agents, DHCP clients, and DHCP snooping-enabled devices. Devices from different vendors may use different DHCP implementation mechanisms. After checking the magic-cookie field in a received DHCP packet, a device may not allow the DHCP packet to pass through and discards the packet. As a result, DHCP becomes unavailable. To solve this problem, you can run the **undo dhcp anti-attack check magic-cookie** command to disable the function of checking the magic-cookie field in a DHCP packet, so that a DHCP packet with an incorrect value in the magic-cookie field can be properly forwarded.

**Prerequisites**

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

## Example

# Disable the function of checking the magic-cookie field in a DHCP packet.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] undo dhcp anti-attack check magic-cookie
```

# 6.3.8 dhcp broadcast suppress enable

## Function

The **dhcp broadcast suppress enable** command enables the DHCP broadcast suppression function.

The **undo dhcp broadcast suppress enable** command disables the DHCP broadcast suppression function.

By default, the DHCP broadcast suppression function is disabled.

## Format

**dhcp broadcast suppress enable**

**undo dhcp broadcast suppress enable**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

If the DHCP relay or DHCP server function is enabled on a VLANIF interface of a device, the DHCP broadcast messages (DHCP Discover and DHCP Request messages) received on the VLANIF interface are broadcast among all the physical interfaces in the corresponding VLAN. If a large number of DHCP clients go online, each physical interface receives a large number of DHCP broadcast messages, affecting the device performance. In this case, you can run the **dhcp broadcast suppress enable** command to enable the DHCP broadcast suppression function, so that the DHCP broadcast messages are not broadcast among the interfaces that do not receive these messages.

**Prerequisites**

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

**Precautions**

In VRRP master/backup scenarios, DHCP broadcast suppression must be disabled so that the backup device can broadcast received DHCP traffic to the master device and IP addresses can be allocated to users through DHCP.

## Example

# Enable the DHCP broadcast suppression function.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp broadcast suppress enable
```

# 6.3.9 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

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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 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 **test** on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcp client class-id test
```

# Set the class-id of a DHCP client to **test** on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] dhcp client class-id test
```

# 6.3.10 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 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-client.options file. By default, the storage device needs to provide more than 80-byte storage space. You can run the **more 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 **test**.

```
<HUAWEI> system-view
[HUAWEI] dhcp client class-id test
```

# 6.3.11 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

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

## Default Level

2: Configuration level

## 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 **test_client** on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcp client client-id test_client
```

# Set the identifier of the DHCP client to **test_client** on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] dhcp client client-id test_client
```

## 6.3.12 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**

### 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

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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 vlanif 100
[HUAWEI-Vlanif100] dhcp client default-route preference 30
```

# In the view of GE0/0/1, set the default route preference that a DHCP server delivers to a DHCP client to 30.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] dhcp client default-route preference 30
```

# 6.3.13 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

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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 server. The server compares the expected lease with the lease in the address pool and assigns a shorter lease to the client.

## Example

# Set the expected lease to 7200s on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcp client expected-lease 7200
```

# Set the expected lease to 7200s on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] dhcp client expected-lease 7200
```

# 6.3.14 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. |

| Parameter | Description | Value |
| --- | --- | --- |
| **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. |

## Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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 VLANIF100 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 vlanif 100
[HUAWEI-Vlanif100] dhcp client gateway-detect period 3600 retransmit 3 timeout 500
```

# Enable gateway detection on GE0/0/1 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 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] dhcp client gateway-detect period 3600 retransmit 3 timeout 500
```

# 6.3.15 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**

## 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

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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 **gateway1** on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcp client hostname gateway1
```

# Set the host name of a DHCP/BOOTP client to **gateway1** on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] dhcp client hostname gateway1
```

# 6.3.16 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

## Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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
```

# Renew the IP address lease on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] dhcp client renew
```

# 6.3.17 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.

By default, the device does not configure the option to be excluded from the DHCP client request list.

## 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

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface

view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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. 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 *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 VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcp client request option-list exclude 3
```

# 6.3.18 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 Option 55 field in DHCP Request packets carries only default request options.

## 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

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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. 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 *Configuration- IP Service Configuration Guide - DHCP Configuration*.

## Example

# Configure the Option55 field in DHCP Request packets to carry option 4 on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcp client request option-list 4
```

# 6.3.19 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.

NOTE

When a device of any of the following models does not work as a DHCP server or DHCP relay, do not configure this command; otherwise, users may go online slowly: S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5720S-LI, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S6720S-S.

## Format

**dhcp enable**

**undo dhcp enable**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

### Usage Scenario

As the network scale expands and the network complexity increases, network configurations become more and more 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.

## Example

# Enable the DHCP function on the device.

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

# 6.3.20 dhcp relay anycast gateway re-route enable

## Function

The **dhcp relay anycast gateway re-route enable** command enables the re-routing function for the DHCP relay agent on a distributed gateway.

The **undo dhcp relay anycast gateway re-route enable** command disables the re-routing function for the DHCP relay agent on a distributed gateway.

By default, the re-routing function for the DHCP relay agent on a distributed gateway is disabled.

NOTE

This command is supported on the following devices: S6730-H, S6730S-H, S6730-S, S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, S5731-H, S6735-S, S6720-EI, S6720S-EI.

## Format

**dhcp relay anycast gateway re-route enable**

**undo dhcp relay anycast gateway re-route enable**

## Parameters

None

## Views

VBDIF interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

In a distributed VXLAN gateway scenario, the DHCP relay function is configured on VBDIF interfaces of distributed gateways. The value of the GIADDR field carried in a request packet sent from a DHCP relay agent to the DHCP server is the IP address of the VBDIF interface. When returning a response packet, the DHCP server figures out the network segment on which the DHCP client resides based on information of this field. However, the response packet from the DHCP server may be forwarded to other distributed gateways (rather than the device that sends the request packet) because IP addresses of VBDIF interfaces on distributed gateways are the same. As a result, the user cannot obtain an IP address.

To resolve the preceding problem, you can enable the re-routing function for DHCP relay agents on VBDIF interfaces of the distributed gateways. After this function is enabled, when a DHCP relay agent sends a request packet, the VTEP IP address of the local device, functioning as the return IP address, is carried in the Option82 field; when a DHCP relay agent returns a response packet, the VTEP IP

address of the local device is also carried in the packet. When processing a response packet from the DHCP server, the DHCP relay agent figures out whether the response packet corresponds to the request packet sent from the local device based on the return IP address carried in the packet. If so, the DHCP relay agent forwards the packet to the client. If not, the DHCP relay agent performs re-routing based on the return IP address to forward the response packet to the corresponding distributed gateway through a VXLAN tunnel.

**Prerequisites**

The DHCP relay function has been enabled using the **dhcp select relay** command in the VBDIF interface view.

**Precautions**

Because the return IP address is carried in the Option82 field, you need to perform the following operations:

1. Run the **dhcp option82 vendor-specific format vendor-sub-option 2 ip-address** *ip-address* command in the system view to use the Sub Option2 field that is customized by the vendor in the Option82 field to carry the VTEP IP address of the local device.
2. Run the **dhcp option82 encapsulation vendor-specific-id** command in the BD view to insert the sub-option customized by the vendor into the Option82 field.
3. Run the **dhcp option82** { **insert** | **rebuild** } **enable** command in the BD view to configure the Option82 field to be inserted into DHCP packets.
4. (Optional) Run the **dhcp relay information enable** command in the VBDIF interface view to enable the Option 82 function for the DHCP relay agent.

## Example

# Enable the re-routing function for the DHCP relay agent on VBDIF100 of a distributed gateway.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] bridge-domain 100
[HUAWEI-bd100] quit
[HUAWEI] interface vbdif 100
[HUAWEI-Vbdif100] dhcp select relay
[HUAWEI-Vbdif100] dhcp relay anycast gateway re-route enable
```

# 6.3.21 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 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 **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
```

# 6.3.22 dhcp relay gateway-switch enable

## Function

The **dhcp relay gateway-switch enable** command enables automatic gateway switching on the DHCP relay agent.

The **undo dhcp relay gateway-switch enable** command disables automatic gateway switching on the DHCP relay agent.

By default, automatic gateway switching is disabled on the DHCP relay agent.

## Format

**dhcp relay gateway-switch enable**

**undo dhcp relay gateway-switch enable**

## Parameters

None

## Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

The **dhcp relay gateway-switch enable** command is used on DHCP relay agents. This command allows a DHCP relay agent to use a secondary IP address as the gateway address to apply for IP addresses for users when it has failed to use the primary IP address to apply for user IP addresses.

**Prerequisites**

DHCP has been enabled globally by using the **dhcp enable** command in the system view. DHCP relay has been enabled on an interface by using the **dhcp select relay** command.

**Precautions**

- After VRRP is configured, if the interface (enabled with DHCP relay) has a primary IP address and several secondary IP addresses, the DHCP relay agent by default uses the virtual IP address first configured for the VRRP group to apply for IP addresses for users. If IP addresses fail to be applied for, the DHCP relay agent tries other virtual IP addresses of the VRRP group one by one based on the VRRP virtual IP address configuration sequence until users successfully obtain IP addresses.
- The DHCP relay agent switches the gateway address from the primary to a secondary IP address only when it has failed to apply an IP address for a user using the primary IP address at least three times and the interval between the first and last failures exceeds 24 seconds.
- Before running this command on an interface, ensure that the interface has a primary IP address and at least one secondary IP address.
- An interface can have a primary IP address and several secondary IP addresses. The system tries the secondary IP addresses one by one based on the IP address configuration sequence until users successfully obtain IP addresses.

## Example

# Enable automatic gateway switching on DHCP relay-enabled VLANIF 10.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ip address 192.168.30.1 255.255.255.0
[HUAWEI-Vlanif10] ip address 192.168.31.1 255.255.255.0 sub
[HUAWEI-Vlanif10] dhcp select relay
[HUAWEI-Vlanif10] dhcp relay server-ip 192.168.20.1
[HUAWEI-Vlanif10] dhcp relay gateway-switch enable
```

# Enable automatic gateway switching on DHCP relay-enabled GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 192.168.30.1 255.255.255.0
[HUAWEI-GigabitEthernet0/0/1] ip address 192.168.31.1 255.255.255.0 sub
[HUAWEI-GigabitEthernet0/0/1] dhcp select relay
[HUAWEI-GigabitEthernet0/0/1] dhcp relay server-ip 192.168.20.1
[HUAWEI-GigabitEthernet0/0/1] dhcp relay gateway-switch enable
```

# 6.3.23 dhcp relay giaddr source-interface

## Function

The **dhcp relay giaddr source-interface** command configures a source interface for relayed DHCP messages and fills the primary IP address of the source interface in the giaddr field of these messages.

The **undo dhcp relay giaddr source-interface** command restores the default configuration.

By default, no source interface for relayed DHCP messages is configured, and the IP address of the DHCP relay agent is filled in the giaddr field of these messages.

NOTE

This command is supported on the following devices: S6730-H, S6730S-H, S6730-S, S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, S5731-H, S6735-S, S6720-EI, S6720S-EI.

## Format

**dhcp relay giaddr source-interface** *interface-type interface-number*

**undo dhcp relay giaddr source-interface**

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *interface-type interface-number* | Specifies a source interface for relayed DHCP messages.<br>• *interface-type* specifies the interface type.<br>• *interface-number* specifies the interface number. | - |

## Views

VBDIF interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

On a network with distributed VXLAN gateways where VBDIF interfaces are enabled with the DHCP relay function, a distributed gateway (as a DHCP relay agent) fills the IP address of its VBDIF interface in the giaddr field of a DHCP DISCOVER message to be sent to DHCP servers. When replying with a DHCP OFFER message, a DHCP server sets the destination IP address to the IP address of the VBDIF interface in the giaddr field carried in its received DHCP DISCOVER message. However, since the IP addresses of VBDIF interfaces on different distributed gateways are the same, the DHCP OFFER message from a DHCP server may be forwarded to a distributed gateway rather than the one relaying the DHCP DISCOVER message received by the server. As a result, the user sending the DHCP DISCOVER message cannot obtain an IP address.

To resolve this issue, you can configure a source interface for relayed DHCP messages on VBDIF interfaces of all distributed gateways. The distributed gateways (as DHCP relay agents) then fill the primary IP address of the specified source interface in the giaddr field of DHCP DISCOVER messages to be relayed to DHCP servers. Since the primary IP address of the source interface configured on each VBDIF interface is unique among all distributed gateways, as long as this IP address is reachable to DHCP servers, the DHCP OFFER messages from DHCP servers can be sent to the correct distributed gateways.

**Prerequisites**

DHCP relay has been enabled using the **dhcp select relay** command in the VBDIF interface view.

**Follow-up Procedure**

By default, a DHCP server selects an IP address from the address pool on the network segment specified in the giaddr field of its received DHCP DISCOVER messages. After this command is run to configure a source interface for relayed DHCP messages on a DHCP relay-enabled interface (which is the gateway for its downlink DHCP clients), the primary IP address of the specified source interface is filled in the giaddr field of DHCP DISCOVER messages destined for DHCP servers. If DHCP servers still select an IP address from the address pool on the network segment specified in the giaddr field, DHCP clients cannot access the network after obtaining IP addresses. This is because the primary IP address of the source interface is on a different network segment from that of the DHCP relay-enabled interface. To resolve the preceding problem, you need to run the **dhcp relay information link-selection insert enable** command to insert the Link-selection sub-option of the Option82 field into relayed DHCP DISCOVER messages, and to fill the IP address of the DHCP relay-enabled interface in the Link-selection suboption. In this case, DHCP servers select IP addresses from the address pool on the network segment specified in the Link-selection sub-option of the Option 82 field of their received DHCP DISCOVER messages.

**Precautions**

- The primary IP address of the source interface for relayed DHCP messages must be reachable to DHCP servers.
- The source interface and VBDIF interfaces enabled with the DHCP relay function can be bound to different VPNs.
- The DHCP server must be able to parse the Link-selection sub-option.

## Example

# On VBDIF 100, configure Loopback 1 as the source interface for relayed DHCP messages.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 1
[HUAWEI-LoopBack1] ip address 10.1.1.1 24
[HUAWEI-LoopBack1] quit
[HUAWEI] dhcp enable
[HUAWEI] bridge-domain 100
[HUAWEI-bd100] quit
[HUAWEI] interface vbdif 100
[HUAWEI-Vbdif100] dhcp select relay
[HUAWEI-Vbdif100] dhcp relay giaddr source-interface loopback 1
```

# 6.3.24 dhcp relay information enable

## Function

The **dhcp relay information enable** command enables the Option 82 function for the DHCP relay agent.

The **undo dhcp relay information enable** command disables the Option 82 function for the DHCP relay agent.

By default, the Option 82 function is disabled for the DHCP relay agent.

## Format

**dhcp relay information enable**

**undo dhcp relay information enable**

## Parameters

None

## Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

This command applies to the DHCP relay agent. When DHCP Request messages carry Option 82 information, the DHCP server can locate user positions accurately and assign IP addresses to users using different policies. After the Option 82 function is enabled on the DHCP relay agent, the device checks the Option 82 field contained in the packets and processes the packets using corresponding policies.

**Prerequisites**

DHCP has been enabled by running the **dhcp enable** command in the system view.

DHCP relay has been enabled by running the **dhcp select relay** command in the interface view.

**Precautions**

If you run the **dhcp relay information enable** command on an interface and the **dhcp option82** { **insert** | **rebuild** } **enable** command in the VLAN view or on a

physical interface in the VLAN simultaneously, only the **dhcp relay information enable** command takes effect.

**Follow-up Tasks**

Run the **dhcp relay information strategy** { **drop** | **keep** | **replace** } command in the interface view to configure strategies for the DHCP relay agent to process Option 82 information.

## Example

# Enable the Option 82 function for the DHCP relay agent on the VLANIF100 interface.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcp select relay
[HUAWEI-Vlanif100] dhcp relay information enable
```

# Enable the Option 82 function for the DHCP relay agent on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] dhcp select relay
[HUAWEI-GigabitEthernet0/0/1] dhcp relay information enable
```

# 6.3.25 dhcp relay information strategy

## Function

The **dhcp relay information strategy** command configures the strategies used by a DHCP relay agent to process Option 82 information.

The **undo dhcp relay information strategy** command restores the default setting.

By default, the strategy used by a DHCP relay agent to process Option 82 information is **replace**.

## Format

**dhcp relay information strategy** { **drop** | **keep** | **replace** }

**undo dhcp relay information strategy**

## Parameters

| Parameters | Description | Value |
| --- | --- | --- |
| **drop** | Configures the DHCP relay agent to drop Option 82 information. | - |

| Parameters | Description | Value |
| --- | --- | --- |
| **keep** | Configures the DHCP relay agent to keep Option 82 information. | - |
| **replace** | Configures the DHCP relay agent to replace Option 82 information. | - |

## Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

This command applies to the DHCP relay agent. When DHCP Request messages carry Option 82 information, the DHCP server can locate user positions accurately and assign IP addresses to users using different policies. When a DHCP relay agent receives DHCP Request messages, it uses one of the following strategies to process Option 82 information:

- Drop:
  - If the received DHCP message does not carry an Option 82 field, the DHCP relay agent forwards the message directly without processing it.
  - If the received DHCP message carries an Option 82 field, the DHCP relay agent drops the Option 82 field and forwards the message.
- Keep:
  - If the received DHCP message does not carry an Option 82 field, the DHCP relay agent forwards the message directly without processing it.
  - If the received DHCP message carries an Option 82 field, the DHCP relay agent keeps the Option 82 field and forwards the message.
- Replace:
  - If the received DHCP message does not carry an Option 82 field, the DHCP relay agent inserts an Option 82 field configured by the administrator into the received message and forwards the message.
  - If the received DHCP message carries an Option 82 field, the DHCP relay agent replaces it with the Option 82 field configured by the administrator and forwards the message.

**Prerequisites**

DHCP has been enabled by running the **dhcp enable** command in the system view.

DHCP relay has been enabled by running the **dhcp select relay** command in the interface view.

The Option 82 function has been enabled for the DHCP relay agent by using the **dhcp relay information enable** command.

## Example

# Configure the DHCP relay agent to drop Option 82 information on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcp select relay
[HUAWEI-Vlanif100] dhcp relay information enable
[HUAWEI-Vlanif100] dhcp relay information strategy drop
```

# Configure the DHCP relay agent to drop Option 82 information on the GE0/0/1 interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] dhcp select relay
[HUAWEI-GigabitEthernet0/0/1] dhcp relay information enable
[HUAWEI-GigabitEthernet0/0/1] dhcp relay information strategy drop
```

# 6.3.26 dhcp relay information link-selection insert enable

## Function

The **dhcp relay information link-selection insert enable** command inserts the Link-selection sub-option of the Option82 field into DHCP messages.

The **undo dhcp relay information link-selection insert enable** command restores the default configuration.

By default, the Link-selection sub-option of the Option82 field is not inserted into DHCP messages.

NOTE

This command is supported on the following devices: S6730-H, S6730S-H, S6730-S, S6730S-S, S5732-H, S5731-S, S5731S-S, S5731S-H, S5731-H, S6735-S, S6720-EI, S6720S-EI.

## Format

**dhcp relay information link-selection insert enable**

**undo dhcp relay information link-selection insert enable**

## Parameters

None

## Views

VBDIF interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

On a network with VXLAN distributed gateways as DHCP relay agents, to ensure that the DHCP OFFER messages from DHCP servers can arrive at the correct distributed gateways, you need to run the **dhcp relay giaddr source-interface** command on the distributed gateways to configure a source interface for relayed DHCP messages and fill the primary IP address of the source interface in the giaddr field. By default, DHCP servers select IP addresses from the address pool on the network segment specified in the giaddr field of their received DHCP DISCOVER messages. After the preceding command is run, since the primary IP address of the source interface is on a different network segment from that of the DHCP relay-enabled interface (which is the gateway for its downlink DHCP clients), if DHCP servers still select IP addresses from the address pool on the network segment specified in the giaddr field, DHCP clients cannot access the network after obtaining IP addresses.

To solve the preceding problem, run the **dhcp relay information link-selection insert enable** command to insert the Link-selection sub-option of the Option82 field into DHCP DISCOVER messages forwarded by the DHCP relay agent, and to fill in the IP address of the DHCP relay-enabled interface in the Link-selection sub-option. In this case, DHCP servers select IP addresses from the address pool on the network segment specified in the Link-selection sub-option of the Option 82 field of their received DHCP DISCOVER messages.

**Prerequisites**

DHCP relay has been enabled using the **dhcp select relay** command in the VBDIF interface view.

**Precautions**

- DHCP servers must be able to parse the Link-selection sub-option.
- After the **dhcp relay information link-selection insert enable** command is run, the Link-selection sub-option is added to DHCP messages, removing the need to configure policies for Option 82 insertion and processing. A DHCP relay agent processes the Link-selection sub-option in different ways depending on the policies for Option 82 insertion and processing:
  - Without policies for Option 82 insertion and processing: The DHCP relay agent inserts the Option 82 field with the Link-selection sub-option into DHCP messages. When forwarding a DHCP message with the Option 82 field, the DHCP relay agent deletes the original Option 82 field and inserts the locally configured Option 82 field with the Link-selection sub-option.
  - With policies for Option 82 insertion and processing: How the DHCP relay agent inserts the Link-selection sub-option into DHCP messages is

determined by the configured policies. For example, if the Option 82 insertion mode is set to **insert**, the DHCP relay agent does not insert the Link-selection sub-option into DHCP messages when receiving DHCP messages carrying the Option 82 field.

You can run the **dhcp option82** { **insert** | **rebuild** } **enable** command to configure the Option 82 insertion mode, and run the **dhcp relay information enable** and **dhcp relay information strategy** { **drop** | **keep** | **replace** } commands to configure an Option 82 processing policy.

## Example

# On VBDIF 100, configure the function of inserting the Link-selection sub-option of the Option82 field into DHCP messages.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] bridge-domain 100
[HUAWEI-bd100] quit
[HUAWEI] interface vbdif 100
[HUAWEI-Vbdif100] dhcp select relay
[HUAWEI-Vbdif100] dhcp relay information link-selection insert enable
```

# 6.3.27 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* ]

## 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. |

| Parameter | Description | Value |
| --- | --- | --- |
| *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 be an existing VPN instance name. |

## Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface 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 IP 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:

- 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.

When multiple DHCP relay agents are connected between the DHCP client and server, this command must be executed on the first DHCP relay agent.

## 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 00e0-fc34-2000.

```
<HUAWEI> system-view
[HUAWEI] dhcp relay release 192.168.1.1 00e0-fc12-3456 10.1.1.1
```

# 6.3.28 dhcp relay request server-match enable

## Function

The **dhcp relay request server-match enable** command configures a DHCP relay agent to check the DHCP server identifier (Option54) in a DHCP Request message to be forwarded.

The **undo dhcp relay request server-match enable** command configures a DHCP relay agent not to check the DHCP server identifier (Option54) in a DHCP Request message to be forwarded.

By default, a DHCP relay agent checks the DHCP server identifier (Option54) in a DHCP Request message to be forwarded.

## Format

**dhcp relay request server-match enable**

**undo dhcp relay request server-match enable**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

During the four-message exchange process, the DHCP Offer message sent by a DHCP server carries the DHCP server identifier (Option54) to identify the server. After receiving the DHCP Offer message, the DHCP client records the DHCP server identifier and carries it in the DHCP Request message to be replied to indicate which DHCP server is selected. When the DHCP relay agent forwards the DHCP Request message, it checks the DHCP server identifier in the message and forwards the message only to the corresponding DHCP server.

If multiple DHCP servers are deployed on the network and the design of a server does not comply with standards, the DHCP server identifier carried in the DHCP Offer message to be sent by the server is not its identifier. As a result, the DHCP server identifier carried in the DHCP Request message is incorrect, the DHCP relay agent forwards the message to an incorrect DHCP server rather than the matching DHCP server, and the client fails to obtain an IP address.

To resolve this issue, you can run the **undo dhcp relay request server-match enable** command, so that the DHCP relay agent does not check the DHCP server identifier (Option54) in the DHCP Request message to be forwarded and forwards the message to all relayed DHCP servers, ensuring that the matching DHCP server can receive the DHCP Request message.

**Prerequisites**

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

## Example

# Configure a DHCP relay agent not to check the DHCP server identifier (Option54) in a DHCP Request message to be forwarded.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] undo dhcp relay request server-match enable
```

# 6.3.29 dhcp relay reply forward all enable

## Function

The **dhcp relay reply forward all enable** command configures a DHCP relay agent to forward all DHCP ACK messages.

The **undo dhcp relay reply forward all enable** command restores the default setting.

By default, a DHCP relay agent forwards only the first received DHCP ACK message.

## Format

**dhcp relay reply forward all enable**

**undo dhcp relay reply forward all enable**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

As defined in RFC2131, the DHCP server that provides only IP addresses for DHCP clients replies with DHCP ACK messages. After receiving a DHCP ACK message, a DHCP relay agent searches for the entry based on the DHCP client's MAC address contained in the message, forwards the message to the corresponding client, and then immediately deletes the entry matching the client.

If multiple DHCP servers are deployed on the network, the design of a server does not comply with standards, and a DHCP client requests for an IP address, the server does not provide an IP address for the DHCP client but replies with a DHCP ACK message. If the DHCP relay agent first receives the DHCP ACK message replied by the server, it incorrectly forwards the message to the client and deletes the corresponding entry. After the DHCP relay agent receives the correct DHCP ACK message, it cannot forward the message because the entry matching the client has been deleted. As a result, the client cannot obtain an IP address.

To resolve this issue, you can run the **dhcp relay reply forward all enable** command, so that the DHCP relay agent does not immediately delete the entry matching a client after forwarding a DHCP ACK message to the client. Instead, the DHCP relay agent deletes the entry that has been aged out to ensure that the subsequently received DHCP ACK messages can be forwarded to the client.

**Prerequisites**

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

## Example

# Configure a DHCP relay agent to forward all DHCP ACK messages.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp relay reply forward all enable
```

# 6.3.30 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 IP address is configured on an interface enabled with DHCP relay.

## Format

**dhcp relay server-ip** [ **vpn-instance** *vpn-name* | **public-net** ] *ip-address*

**undo dhcp relay server-ip** { [ **vpn-instance** *vpn-name* | **public-net** ] *ip-address* | **all** }

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **vpn-instance** *vpn-name* | Specifies the name of a VPN instance. | The value must be the name of an existing VPN instance. |
| **public-net** | Indicates that the public network is used to forward packets. | - |
| *ip-address* | Specifies the IP address of a DHCP server. | The value is in dotted decimal notation. |
| **all** | Deletes all the DHCP server IP addresses configured on an interface. | - |

## Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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 IP address on the DHCP relay agent. If the DHCP server and DHCP client are not in the same VPN, you also need to specify the VPN where the DHCP server resides.

When a DHCP relay agent forwards a DHCP DISCOVER message, it does not check whether the DHCP server 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 **ip relay address cycle** command to reduce the number of messages 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**

To configure multiple DHCP server IP addresses, run this command for multiple times.

Each interface enabled with DHCP relay can be configured with a maximum of 20 DHCP server IP addresses.

If the interface enabled with DHCP relay is bound to a VPN instance but no VPN instance is specified for the DHCP server served by the DHCP relay agent, the DHCP relay agent sends packets through the VPN instance to which the interface belongs by default. If a VPN instance is specified for the DHCP server, the DHCP relay agent sends packets through the VPN instance specified for the DHCP server.

## Example

# Configure DHCP relay and three DHCP server IP addresses on VLANIF 10.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] dhcp select relay
[HUAWEI-Vlanif10] dhcp relay server-ip 10.1.1.2
[HUAWEI-Vlanif10] dhcp relay server-ip vpn-instance temp 10.1.1.3
[HUAWEI-Vlanif10] dhcp relay server-ip public-net 192.0.2.1
```

# Configure DHCP relay and three DHCP server IP addresses on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
```

```
[HUAWEI-GigabitEthernet0/0/1] dhcp select relay
[HUAWEI-GigabitEthernet0/0/1] dhcp relay server-ip 10.1.1.2
[HUAWEI-GigabitEthernet0/0/1] dhcp relay server-ip vpn-instance temp 10.1.1.3
[HUAWEI-GigabitEthernet0/0/1] dhcp relay server-ip public-net 192.0.2.1
```

# 6.3.31 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

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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**

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.
- 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.

## Example

# Configure the DHCP server group of a DHCP relay agent as **group1** on VLANIF100.

```
<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 vlanif 100
[HUAWEI-Vlanif100] dhcp select relay
[HUAWEI-Vlanif100] dhcp relay server-select group1
```

# Configure the DHCP server group of a DHCP relay agent as **group1** on GE0/0/1.

```
<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 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] dhcp select relay
[HUAWEI-GigabitEthernet0/0/1] dhcp relay server-select group1
```

# 6.3.32 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**

## 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
```

# 6.3.33 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

## Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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.

**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.

## Example

# Enable VLANIF100 to use the global address pool.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 24
[HUAWEI-Vlanif100] dhcp select global
```

# Enable GE0/0/1 to use the global address pool.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.1.1.1 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select global
```

# 6.3.34 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

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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.

**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.

## Example

# Enable VLANIF100 to use the interface address pool.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.2 24
[HUAWEI-Vlanif100] dhcp select interface
```

# Enable GE0/0/1 to use the interface address pool.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.1.1.2 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
```

# 6.3.35 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

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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 **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 **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.
- 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.

## Example

# Enable the DHCP relay function on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcp select relay
```

# Enable the DHCP relay function on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] dhcp select relay
```

# 6.3.36 dhcp server alarm ip-used percentage

## Function

The **dhcp server alarm ip-used percentage** command configures the percentage of used addresses in an interface address pool at which an address exhaustion alarm is generated and the percentage at which the alarm is cleared.

The **undo dhcp server alarm ip-used percentage** command restores the default percentage of used addresses in an interface address pool at which an address

exhaustion alarm is generated and the default percentage at which the alarm is cleared.

By default, an alarm is generated when the percentage of used addresses in an interface address pool reaches 100%, and the alarm is cleared when the percentage is 50%.

## Format

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

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

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *alarm-resume-percentage* | Specifies the percentage of used addresses in an interface address pool at which an address exhaustion alarm is cleared. | The value is an integer that ranges from 1 to 100. The default value is 50.<br>**NOTE**<br>The percentage of used addresses in an interface address pool at which the address exhaustion alarm is cleared cannot exceed the percentage at which an address exhaustion alarm is generated. |
| *alarm-percentage* | Specifies the percentage of used addresses in an interface address pool at which an address exhaustion alarm is generated. | The value is an integer that ranges from 1 to 100. The default value is 100. |

## Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

When the addresses in an interface address pool are used up, an address exhaustion alarm is generated to notify the administrator. The alarms corresponding to this command are as follows:

- When the number of used IP addresses in an IP address pool reaches the alarm threshold, the alarm hwUsedIPReachThreshold with ID 1.3.6.1.4.1.2011.6.8.2.2.0.6 is generated.
- When the number of used IP addresses in an IP address pool falls below the alarm clear threshold, the alarm hwUsedIPReachThresholdResume with the ID 1.3.6.1.4.1.2011.6.8.2.2.0.7 is generated.

**Prerequisites**

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

**Precautions**

The percentage of used addresses in an interface address pool at which the address exhaustion alarm is cleared cannot exceed the percentage at which an address exhaustion alarm is generated.

## Example

# Configure the percentage of used IP addresses in the interface address pool of VLANIF 100 at which an address exhaustion alarm is generated and the percentage at which the alarm is cleared.

```
<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
```

# Configure the percentage of used IP addresses in the interface address pool of GE0/0/1 at which an address exhaustion alarm is generated and the percentage at which the alarm is cleared.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.10.10.10 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server alarm ip-used percentage 80 90
```

# 6.3.37 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**

## 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. When double quotation marks are used around the string, spaces are allowed in the string. |

## Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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 **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.

3. The DHCP server function has been enabled on the interface using the **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
```

# Configure the name of the startup configuration file as **start.ini** for the DHCP client on the GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 192.168.1.1 255.255.255.0
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server bootfile start.ini
```

# 6.3.38 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 does not respond 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
```

# 6.3.39 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 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
```

# 6.3.40 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. |
| **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

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. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.
3. 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
```

# Enable automatic reclaim for conflicting IP addresses in the address pool on GE0/0/1, and set the interval for automatic reclaim to one day.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 192.168.1.1 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server conflict auto-recycle interval day 1
```

## 6.3.41 dhcp server database

### Function

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

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 7200 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 **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.

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.
- During the interval, if the device restarts unexpectedly, DHCP data generated at the interval is lost. Users can only recover the last successfully saved DHCP data from storage device files.

## 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
```

# 6.3.42 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 from 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** }

## 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

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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 DNS 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**

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.
3. 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.

## Example

# Specify a DNS server at 10.10.1.254 for domain name resolution when IP addresses in the interface address pool on VLANIF100 are assigned to clients.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 24
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server dns-list 10.10.1.254
```

# Specify a DNS server at 192.168.1.254 for domain name resolution when IP addresses in the interface address pool on GE0/0/1 are assigned to clients.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.10.10.10 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server dns-list 192.168.1.254
```

# 6.3.43 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.<br>**NOTE**<br>When quotation marks are used around the string, spaces are allowed in the string. |

## Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

## Default Level

2: Configuration level

## 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

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

### Precautions

If no domain name is specified for an interface address pool, a DHCP server does not send a domain name to clients, and users cannot access the Web service by using a domain name.

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 vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 24
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server domain-name example.com
```

# Specify the domain name in the address pool on GE0/0/1 as **example.com**.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.10.10.10 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server domain-name example.com
```

# 6.3.44 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 an interface address pool.

By default, all IP addresses in an 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* ]

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *start-ip-address* | Specifies the start IP address of the IP address segment where addresses cannot be automatically assigned to clients. | The value is in dotted decimal notation. |

| Parameter | Description | Value |
| --- | --- | --- |
| *end-ip-address* | Specifies the end IP address of the IP address segment where addresses cannot be automatically assigned to clients. If *end-ip-address* is not specified, only the IP address corresponding to *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

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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 such IP address conflicts, you need to exclude these IP addresses from being automatically assigned 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**

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.

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

**Precautions**

- IP addresses that cannot be automatically assigned must be in the address pool. If IP address range 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 new IP address range.
- You do not need to exclude the gateway address configured using the **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 status of the interface IP address to Conflict during address assignment.
- If you run this command multiple times, you can specify multiple IP addresses or ranges of IP addresses that cannot be automatically assigned to clients from the specified address pool.
- You can run the **display ip pool** command to check the IP addresses in use in the current address pool, so that you can exclude the unused IP addresses from being automatically assigned to clients. If you need to exclude IP addresses in Used and Conflict states from being automatically assigned to clients after address reclamation, you can also run the **excluded-ip-address** command. If an IP address has been bound to a specific MAC address, adding the IP address to the IP address list in which IP addresses are not automatically assigned to clients will unbind the IP address from the MAC address.

## Example

# Disable IP addresses 192.168.1.1 to 192.168.1.20 from being automatically assigned to clients from the address pool on 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 excluded-ip-address 192.168.1.1 192.168.1.20
```

# Disable IP address 192.168.1.30 in Used state from being automatically assigned to clients from the address pool on 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 excluded-ip-address 192.168.1.30
Warning: The address is in used or conflict state. Are you sure to continue excluding the address?[Y/N]:y
```

# Disable IP addresses 10.10.10.11 to 10.10.10.20 from being automatically assigned to clients from the address pool on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.10.10.10 24
```

```
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server excluded-ip-address 10.10.10.11 10.10.10.20
```

# 6.3.45 dhcp server force insert option

## 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

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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.

**Prerequisites**

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.
3. The DHCP server function has been enabled on the interface using the **dhcp select interface** command.
4. 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 VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server option 4 hex 11 22
[HUAWEI-Vlanif100] dhcp server force insert option 4
```

# Configure a DHCP server to forcibly insert Option 4 to a DHCP Response packet on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server option 4 hex 11 22
[HUAWEI-GigabitEthernet0/0/1] dhcp server force insert option 4
```

# 6.3.46 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 disables the function of forcing a DHCP server to reply with a DHCP NAK message.

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

## 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
```

# 6.3.47 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** }

## 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

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

## Default Level

2: Configuration level

## Usage Guidelines

### Usage Scenario

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

NOTICE

The default gateway address allocated to the DHCP client can only be a class A, B, or C address, and cannot be a broadcast address, a host address, or a class A address whose network address is 0.

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.

**Prerequisites**

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

## Example

# Enable a DHCP server on a VLANIF100 to pre-allocate default gateway address 10.1.1.1 to DHCP clients.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 24
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server gateway-list 10.1.1.1
```

# Enable a DHCP server on GE0/0/1 to pre-allocate default gateway address 10.1.1.1 to DHCP clients.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.1.1.1 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server gateway-list 10.1.1.1
```

# 6.3.48 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*

## 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. 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 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 **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 32 DHCP server groups in the system, and a maximum of 20 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
```

# 6.3.49 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

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

## Default Level

2: Configuration level

## Usage Guidelines

### 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

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

## Example

# Enable a DHCP server on a VLANIF100 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 vlanif 100
[HUAWEI-Vlanif100] ip address 192.168.1.1 24
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server ip-range 192.168.1.2 192.168.1.100
```

# Enable a DHCP server on GE0/0/1 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 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 192.168.1.1 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server ip-range 192.168.1.2 192.168.1.100
```

# 6.3.50 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. |

| 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

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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. In scenarios with high user mobility, new clients may fail to obtain IP addresses if allocated addresses are not reclaimed for a long time. As such, shortening the DHCP lease is recommended. For example, in Wi-Fi access scenarios of an airport or station, you can change the DHCP lease to 30 minutes.

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 **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**

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.
3. 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 VLANIF100 to 2 days 2 hours and 30 minutes.

```
<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 lease day 2 hour 2 minute 30
```

# Set the IP address lease of the address pool on GE0/0/1 to 2 days 2 hours and 30 minutes.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.10.10.10 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server lease day 2 hour 2 minute 30
```

# 6.3.51 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** ] *

## 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

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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**

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

**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 in the *CLI-based Configuration - Device Management Configuration Guide*.

  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
```

# Enable the logging function during IP address allocation of the DHCP server on the interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 192.168.1.1 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server logging
```

# 6.3.52 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**

## 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

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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

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

## Example

# Set the subnet mask of IP addresses that a DHCP server on a VLANIF100 pre-allocates to DHCP clients to 255.255.255.0.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 24
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server mask 255.255.255.0
```

# Set the subnet mask of IP addresses that a DHCP server on GE0/0/1 pre-allocates to DHCP clients to 255.255.255.0.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.1.1.1 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server mask 255.255.255.0
```

# 6.3.53 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.

## 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

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.
3. 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 VLANIF100 are assigned to clients.

```
<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 nbns-list 192.168.1.99
```

# Specify a NetBIOS server at 192.168.1.99 for domain name resolution when IP addresses in the interface address pool on GE0/0/1 are assigned to clients.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.10.10.10 24
```

```
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server nbns-list 192.168.1.99
```

# 6.3.54 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. | - |
| **p-node** | Indicates a node in peer-to-peer mode. This node obtains mappings by communicating with the NetBIOS server. | - |

## Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE

interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.
3. 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 VLANIF100 to **p-node**.

```
<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 netbios-type p-node
```

# Set the NetBIOS node type for a client in the address pool on GE0/0/1 to **p-node**.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.10.10.10 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server netbios-type p-node
```

# 6.3.55 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

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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**

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.
3. 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 who 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
```

# Specify the server IP address 192.168.1.2 in the interface address pool on GE0/0/1 used to provide services for terminal users.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.1.1.2 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server next-server 192.168.1.2
```

# 6.3.56 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* ] ]

## 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.<br>**NOTE**<br>• The format of option82, Option121 and Option184 are different from the other codes of a customized option.<br>• There are well-known options and customized options. For details about well-known options, see RFC 2132.<br>• When the switch functions as a DHCP client, Option 148 can be used in an EasyDeploy scenario and is not recommended in other scenarios. |
| **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. |

| Parameter | Description | Value |
| --- | --- | --- |
| **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). |
| **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.<br>• The character string in explicit text is a string of 1 to 64 characters.<br>• The character string in cipher text is a string of 32 to 104 characters.<br>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

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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**

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.
3. 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 eight 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.
- When users on an enterprise's intranet use a proxy server to connect to the Internet, you need to configure proxy server parameters so that users can use browsers to access the network. The Web Proxy Auto-Discovery Protocol (WPAD) implements automatic configuration of these parameters. The administrator does not need to manually configure these parameters on each client. To implement the WPAD function, the administrator needs to deploy the configuration file of the proxy server in advance, and then run the **dhcp server option 252 ascii** *ascii-string* command to specify the URL of the configuration file. The *ascii-string* parameter specifies the URL of the configuration file, in the format of https://*xxx*/proxy.pac. Set *ascii-string* according to the actual location of the configuration file. When a browser accesses the network, the browser requests the DHCP server to send the URL of the configuration file on the proxy server, and then downloads the configuration file to conduct automatic configuration. After the configuration is completed, the browser can access the network.

NOTE

The value of *ascii-string* cannot be enclosed in double quotation marks as "*ascii-string*". Otherwise, terminals cannot parse Option252.

## Example

# Set Option64 to 0x11 (a hexadecimal number) for the interface address pool on 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 option 64 hex 11
```

# Set Option64 to 0x11 (a hexadecimal number) for the interface address pool on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.10.10.10 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server option 64 hex 11
```

# 6.3.57 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* ]

## 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

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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.

**Prerequisites**

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.
3. The DHCP server function has been enabled on the interface using the **dhcp select interface** command.
4. 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
```

# Configure a classless static route allocated by a DHCP server to a client in the interface address pool on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.1.1.2 24
```

```
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server option121 ip-address 10.10.10.10 24 192.168.11.11
```

# 6.3.58 dhcp server option125 vendor-specific

## Function

The **dhcp server option125 vendor-specific** command configures the vendor ID in Option 125 delivered by a DHCP server to a client.

The **undo dhcp server option125 vendor-specific** command deletes the vendor ID in Option 125 delivered by a DHCP server to a client.

By default, no vendor ID is configured in Option 125 delivered by a DHCP server to a client.

## Format

**dhcp server option125 vendor-specific** *vendor-id*

**undo dhcp server option125 vendor-specific**

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *vendor-id* | Indicates the vendor ID, which is assigned by the IANA. 2011 indicates Huawei. | The value is an integer in the range from 1 to 4294967295. |

## Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

## Default Level

2: Configuration level

## Usage Guidelines

### Usage Scenario

If a DHCP client sends a DHCP Discover message carrying a vendor ID to a DHCP server, the DHCP server needs to exchange the vendor information with the client using Option 125. You can run the **dhcp server option 125** [ **sub-option** *sub-code* ] **ascii** *ascii-string* command to configure the vendor ID in Option 125 delivered by a DHCP server to a client. However, it is complex to convert the vendor ID into an ASCII character string.

To simplify the configuration, you can run the **dhcp server option125 vendor-specific** *vendor-id* command to specify the vendor ID in Option 125 of packets sent from a DHCP server to a client.

**Prerequisites**

1. IP addresses have been configured in an interface address pool using the **ip address** command.
2. The DHCP server function has been enabled on the interface using the **dhcp select interface** command.
3. Fields except **Vendor-ID** in Option 125 have been configured for the interface address pool using the **dhcp server option 125 ascii** *ascii-string* command. The **Vendor-ID** field in Option 125 occupies four bytes. Therefore, the *ascii-string* value is a string of 1 to 251 bytes.
4. (Optional) The **dhcp server force insert option 125** command has been used to configure the DHCP server to insert the Option 125 field specified for the interface address pool into the DHCP response packet sent from a DHCP server to a client. This resolves the problem in the following situation: The device functions as a DHCP server, and the DHCP request packet sent by a DHCP client does not carry Option 125. However, the DHCP client still expects the DHCP server to deliver Option 125 configured for the interface address pool.

**Precautions**

This command and the **dhcp server option 125 sub-option** *sub-code* **ascii** *ascii-string* are mutually exclusive on an interface.

## Example

# Configure the VLAN and vendor information in Option 125 for the interface address pool on VLANIF 100.

```
<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 option 125 ascii id:vlan=100
[HUAWEI-Vlanif100] dhcp server option125 vendor-specific 2011
```

# Configure the VLAN and vendor information in Option 125 for the interface address pool on GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.1.1.2 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server option 125 ascii id:vlan=10
[HUAWEI-GigabitEthernet0/0/1] dhcp server option125 vendor-specific 2011
```

# 6.3.59 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** ]

## 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

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

## Default Level

2: Configuration level

## Usage Guidelines

### Usage Scenario

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.

### Prerequisites

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

## 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
```

# Configure Option 184 allocated by a DHCP server to a client in the interface address pool on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.1.1.2 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server option184 as-ip 10.10.10.10
```

# 6.3.60 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. |

| 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
```

# 6.3.61 dhcp server sip-server

## 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

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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.

**Prerequisites**

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

**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.

## 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 vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 24
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server sip-server ip-address 10.1.1.1
```

# Specify 10.1.1.1 as the IP address of the SIP server when addresses in the interface GE0/0/1 address pool are assigned to clients.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.1.1.1 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server sip-server ip-address 10.1.1.1
```

# 6.3.62 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. When double quotation marks are used around the string, spaces are allowed in the string. |

## Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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 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 **dhcp enable** command in the system view.
2. IP addresses in the interface address pool have been configured using the **ip address** command.
3. The DHCP server function has been enabled on the interface using the **dhcp select interface** command.
4. The startup configuration file name has been configured for the DHCP client using the **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 **Test** in the interface address pool on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 255.255.255.0
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server bootfile start.ini
[HUAWEI-Vlanif100] dhcp server sname Test
```

# Configure the name of the server where the DHCP client obtains the startup configuration file as **Test** in the interface address pool on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.1.1.1 255.255.255.0
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server bootfile start.ini
[HUAWEI-GigabitEthernet0/0/1] dhcp server sname Test
```

# 6.3.63 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* ]

## 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. |

| Parameter | Description | Value |
| --- | --- | --- |
| **mac-address** *mac-address* | Specifies the user MAC address. | The value is in H-H-H format. An H is a hexadecimal number of 1 to 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

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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**

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

**Precautions**

- Ensure that the bound IP address is not configured as the IP address that cannot be allocated using the **dhcp server excluded-ip-address** command.
- 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. 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 vlanif 100 to a host with the MAC address 00e0-fcf3-2a3b.

```
<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 static-bind ip-address 10.10.10.20 mac-address 00e0-fcf3-2a3b
```

# Configure a DHCP server to assign a fixed IP address 10.10.10.20 in the interface address pool on GE0/0/1 to a host with the MAC address 00e0-fcf3-2a3b.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address 10.10.10.10 24
[HUAWEI-GigabitEthernet0/0/1] dhcp select interface
[HUAWEI-GigabitEthernet0/0/1] dhcp server static-bind ip-address 10.10.10.20 mac-address 00e0-
fcf3-2a3b
```

# 6.3.64 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**

## 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
```

# 6.3.65 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** [ **vpn-instance** *vpn-name* | **public-net** ] *ip-address* [ *ip-address-index* ]

**undo dhcp-server** { [ **vpn-instance** *vpn-name* | **public-net** ] *ip-address* | *ip-address-index* }

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **vpn-instance** *vpn-name* | Specifies the name of a VPN instance. | The value must be the name of an existing VPN instance. |
| **public-net** | Indicates that the public network is used to forward packets. | - |
| *ip-address* | Specifies the IP address of a DHCP server. | The value is in dotted decimal notation. |
| *ip-address-index* | Specifies an index for a DHCP server 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 19. |

## 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 20 DHCP servers. You can delete a DHCP server by specifying *ip-address-index*.
- If a VPN instance is bound to an interface, the DHCP server group must be bound to this VPN instance.
- If the interface enabled with DHCP relay is bound to a VPN instance but no VPN instance is specified for a DHCP server in a DHCP server group, the DHCP relay agent sends packets through the VPN instance to which the interface belongs by default. If a VPN instance is specified for a DHCP server in a DHCP server group, the DHCP relay agent sends packets through the VPN instance specified for the DHCP server.

## Example

# Add the DHCP server at 10.10.78.56 to the 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
```

# 6.3.66 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**

## 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.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp set ttl 16
```

# 6.3.67 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 6-16** and **Table 6-17** list the mapping between the DHCP packet rate and CPU/memory usage after dynamic rate limiting on DHCP packets is enabled.

**Table 6-16** DHCP packet rate and CPU usage

| CPU Usage (%) | DHCP Packet Rate (packets/second) |
| --- | --- |
| (70–85) | 100 |
| [85–100) | 50 |
| 100 | 10 |

**Table 6-17** 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
```

# 6.3.68 dhcp udp-checksum enable

## Function

The **dhcp udp-checksum enable** command enables a device to add the UDP header checksum to DHCP packets to be sent.

The **undo dhcp udp-checksum enable** command disables a device from adding the UDP header checksum to DHCP packets to be sent.

By default, the UDP header checksum carried in DHCP packets sent by a device is 0, and the peer device does not verify the checksum.

## Format

**dhcp udp-checksum enable**

**undo dhcp udp-checksum enable**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

If the peer device does not comply with protocol standards, the peer device still verifies the UDP header checksum when the checksum carried in DHCP packets is 0. In this case, you can run the **dhcp udp-checksum enable** command to enable the device to add the UDP header checksum to DHCP packets to be sent.

**Prerequisites**

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

**Precautions**

A device can add the UDP header checksum to DHCP packets to be sent only if the device functions as a DHCP server.

## Example

# Enable a device to add the UDP header checksum to DHCP packets to be sent.

```
<HUAWEI> system-view
[HUAWEI] dhcp udp-checksum enable
```

# 6.3.69 display dhcp client

## Function

The **display dhcp client** command displays DHCP/BOOTP client lease information.

## 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:<br>• *interface-type*: specifies the interface type.<br>• *interface-number*: specifies the number of the interface. | - |

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

When a device functions as a DHCP/BOOTP client, you can run this command to view DHCP/BOOTP client lease information.

## Example

# Display DHCP client lease information.

```
<HUAWEI> display dhcp client
DHCP client lease information on interface Vlanif119 :
 Current machine state         : Bound
 Internet address assigned via : DHCP
 Physical address              : 00e0-fccd-a896
 IP address                    : 192.168.119.254
 Subnet mask                   : 255.255.255.0
 Gateway ip address            : 192.168.119.1
                                 192.168.119.3
                                 192.168.119.2
 DHCP server                   : 192.168.119.1
 Lease obtained at             : 2008-10-01 04:35:10
 Lease expires at              : 2008-10-01 04:36:10
 Lease renews at               : 2008-10-01 04:35:40
 Lease rebinds at              : 2008-10-01 04:36:03
 Classless static route        : 192.168.0.0/16 via 192.168.119.1
                                 10.10.0.0/16 via 192.168.119.2
```

```
Host name              : client   Request option list      : 1 3 6 15 28 33 44 121 184
Class identifier       : huawei
Client identifier      : 00e0-fccd-a896
```

**Table 6-18** 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. The value can be:<br>• **Halt**: indicates the state of stopping applying for IP addresses.<br>• **Init**: indicates the initialization state.<br>• **Waiting offer**: indicates the state of waiting for an OFFER message.<br>• **Selecting**: indicates the state that the state machine enters after DHCP DISCOVER messages are sent to search for DHCP servers. In this state, the device is waiting for response messages from DHCP servers.<br>• **Requesting**: indicates the state that the state machine enters after DHCP REQUEST messages are sent to request IP addresses. In this state, the device is waiting for response messages from DHCP servers.<br>• **Bound**: indicates the state that the state machine enters after the device successfully obtains an IP address by receiving the DHCP ACK message from a DHCP server.<br>• **Renewing**: indicates the state that the state machine enters after T1 timer times out.<br>• **Rebind**: indicates the state that the state machine enters after T2 timer times out. |
| Internet address assigned via | Indicates that the device IP address is obtained through DHCP or BOOTP. |
| Physical address | Device MAC address. |
| IP address | Device IP address. |
| Subnet mask | Mask of the device IP address. |

| Item | Description |
| --- | --- |
| Gateway ip address | Gateway address of the DHCP or BOOTP server. |
| DHCP server | IP address of the DHCP server (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 | Lease renewal timer, which is 50% of the lease (no value for a BOOTP client). |
| Lease rebinds at | Rebinding timer, which is 87.5% of the lease (no value for a BOOTP client). |
| Classless static route | Classless static route. |
| Host name | Information in Option 12, which is the host name of the client. |
| Request option list | Information in Option 55, which is the parameter list requested by the client. |
| Class identifier | Information in Option 60, which is the vendor class identifier of the client. |
| Client identifier | Information in Option 61, which is the client identifier. |

# 6.3.70 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* ]

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **interface** *interface-type interface-number* | Displays packet statistics on a specified interface of the DHCP/BOOTP client:<br>• *interface-type* specifies the interface type.<br>• *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 GigabitEthernet0/0/1GigabitEthernet0/0/1 :
Input: total 0 packets
  Bootp reply            :         0
  Offer                  :         0
  Ack                    :         0
  Nak                    :         0
  Dropped untrusted reply :          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 6-19** Description of the **display dhcp client statistics** command output

| Item | Description |
| --- | --- |
| Input | Total number of DHCP messages received by the client. |
| 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. |
| Dropped untrusted reply | Number of untrusted reply messages discarded by the device. |
| 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. |

# 6.3.71 display dhcp configuration

## Function

The **display dhcp configuration** command displays the configuration of a DHCP public module.

## Format

**display dhcp configuration**

## Parameters

None

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

You can run this command to check the configuration of a DHCP public module.

## Example

# Display the configuration of a DHCP public module.

```
<HUAWEI> display dhcp configuration
  DHCP global running information :
  DHCP                                  : Enable
  DHCP speed limit                      : Disable  (default)
  DHCP anti-attack check duplicate option     : Disable  (default)
  DHCP broadcast suppress               : Disable  (default)
  DHCP anti-attack check udp-checksum         : Enable   (default)
  DHCP anti-attack check magic-cookie         : Disable  (default)
  DHCP udp-checksum                     : Disable  (default)
```

**Table 6-20** Description of the **display dhcp configuration** command output

| Item | Description |
| --- | --- |
| DHCP global running information | Global configuration of a DHCP public module. |

| Item | Description |
| --- | --- |
| DHCP | Whether DHCP is enabled. The value can be:<br>● Enable: DHCP is enabled.<br>● Disable (default): DHCP is disabled. By default, DHCP is disabled.<br>To configure this parameter, run the **dhcp enable** command. |
| DHCP speed limit | Whether dynamic DHCP packet rate limiting is enabled. The value can be:<br>● Enable: This function is enabled.<br>● Disable (default): This function is disabled. By default, dynamic DHCP packet rate limiting is disabled.<br>To configure this parameter, run the **dhcp speed-limit auto** command. |
| DHCP anti-attack check duplicate option | Whether the function of checking and discarding DHCP packets with duplicate options is enabled. The value can be:<br>● Enable: This function is enabled.<br>● Disable (default): This function is disabled. By default, the function of checking and discarding DHCP packets with duplicate options is disabled.<br>To configure this parameter, run the **dhcp anti-attack check duplicate option** command. |
| DHCP broadcast suppress | Whether DHCP broadcast suppression is enabled. The value can be:<br>● Enable: This function is enabled.<br>● Disable (default): This function is disabled. By default, DHCP broadcast suppression is disabled.<br>To configure this parameter, run the **dhcp broadcast suppress enable** command. |

| Item | Description |
| --- | --- |
| DHCP anti-attack check udp-checksum | Whether the function of checking the UDP header checksum in a DHCP packet and discarding a DHCP packet with an incorrect checksum is enabled. The value can be:<br>● Enable (default): This function is enabled. By default, a device checks the UDP header checksum in a DHCP packet and discards a DHCP packet with an incorrect checksum.<br>● Disable: This function is disabled.<br>To configure this parameter, run the **dhcp anti-attack check duplicate option** command. |
| DHCP anti-attack check magic-cookie | Whether the function of checking the magic cookie field in a DHCP packet and discarding a DHCP packet with an incorrect magic cookie field value is enabled. The value can be:<br>● Enable: This function is enabled.<br>● Disable (default): This function is disabled. By default, a device does not check the magic cookie field in a DHCP packet but directly forwards a DHCP packet with an incorrect magic cookie field value.<br>To configure this parameter, run the **dhcp anti-attack check magic-cookie** command. |
| DHCP udp-checksum | Whether a device is enabled to add the UDP header checksum to DHCP packets to be sent. The value can be:<br>● Enable: The device is enabled to add the UDP header checksum to DHCP packets to be sent.<br>● Disable (default): The device is disabled from adding the UDP header checksum to DHCP packets to be sent. By default, the UDP header checksum carried in DHCP packets sent by a device is 0, and the peer device does not verify the checksum.<br>To configure this parameter, run the **dhcp udp-checksum enable** command. |

# 6.3.72 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, 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    : example.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    : example.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 6-21** Description of the **display dhcp option template** command output

| Item | Description |
| --- | --- |
| Template-Name | Name of the DHCP Option template.<br>To specify the parameter, run the **dhcp option template** command. |
| Template-No | Index value of the DHCP Option template. |
| Next-server | IP address of a server configured for the client after the client automatically obtains the IP address.<br>To specify the parameter, run the **next-server** command in the DHCP Option template view. |
| Domain-name | Name of a domain.<br>To specify the parameter, run the **domain-name** command in the DHCP Option template view. |
| Option-code | Code for a customized option.<br>To specify the parameter, run the **option** command in the DHCP Option template view. |

| Item | Description |
| --- | --- |
| Option-subcode | Code for a customized sub-option.<br>To specify the parameter, run the **option** command in the DHCP Option template view. |
| Option-type | Character string type for a customized option.<br>To specify the parameter, run the **option** command in the DHCP Option template view. |
| Option-value | Character string value for a customized option.<br>To specify the parameter, run the **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.<br>To specify the parameter, run the **dns-list** command in the DHCP Option template view. |
| 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.<br>To specify the parameter, run the **nbns-list** command in the DHCP Option template view. |
| Netbios-type | NetBIOS node type.<br>To specify the parameter, run the **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.<br>To specify the parameter, run the **gateway-list** command in the DHCP Option template view. |

# 6.3.73 display dhcp relay

## Function

The **display dhcp relay** command displays configuration information about a DHCP relay agent.

## Format

**display dhcp relay** { **configuration** | **all** | **interface** *interface-type interface-number* }

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **configuration** | Displays configuration information about DHCP relay agents configured globally and on all interfaces. | - |
| **all** | Displays configuration information about DHCP relay agents configured on all interfaces. | - |
| **interface** *interface-type interface-number* | Displays configuration information about a DHCP relay agent configured on a specified interface.<br>• *interface-type* specifies the interface type.<br>• *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 globally and on interfaces.

## Example

# Display configuration information about DHCP relay agents on all interfaces.

```
<HUAWEI> display dhcp relay configuration
  DHCP relay global running information :
  DHCP relay address cycle           : Disable (default)
  DHCP relay trust option82          : Enable  (default)
  DHCP relay request server-match    : Enable  (default)
  DHCP relay reply forward all       : Disable (default)
 DHCP relay agent running information of interface
Vbdif100 :
 Server IP address [00] : 10.1.1.1
 Gateway address in use : 10.10.1.10
 Anycast gateway re-route: disable
 GIADDR source interface : LoopBack1
 Link-selection insert  : enable
 DHCP relay agent running information of interface Vlanif5 :
 Server group name      : group1
 Gateway address in use : 10.100.100.1
 Gateway switch         : enable
 DHCP relay agent running information of interface Vlanif100 :
 Server IP address [00] : 10.2.2.3
 VPN instance      [00] : vpn1
 Gateway address in use : 10.2.2.2
```

**Table 6-22** Description of the **display dhcp relay configuration** command output

| Item | Description |
| --- | --- |
| DHCP relay global running information | Configuration information about DHCP relay agents configured globally. |
| DHCP relay address cycle | Whether the DHCP server polling function is enabled on a DHCP relay agent.<br>• Enable: The DHCP server polling function is enabled on a DHCP relay agent.<br>• Disable: The DHCP server polling function is disabled on a DHCP relay agent.<br>To configure this item, run the **ip relay address cycle** command. |
| DHCP relay trust option82 | Whether Option 82 is enabled on a DHCP relay agent.<br>• Enable: Option 82 is enabled on a DHCP relay agent.<br>• Disable: Option 82 is disabled on a DHCP relay agent.<br>To configure this item, run the **dhcp relay trust option82** command. |

| Item | Description |
| --- | --- |
| DHCP relay request server-match | Whether a DHCP relay agent is enabled to check the DHCP server identifier (Option54) in a DHCP Request message to be forwarded.<br>• Enable: A DHCP relay agent is enabled to check the DHCP server identifier (Option54) in a DHCP Request message to be forwarded.<br>• Disable: A DHCP relay agent is disabled from checking the DHCP server identifier (Option54) in a DHCP Request message to be forwarded.<br>To configure this item, run the **dhcp relay request server-match enable** command. |
| DHCP relay reply forward all | Whether a DHCP relay agent is enabled to forward all DHCP ACK messages.<br>• Enable: A DHCP relay agent is enabled to forward all DHCP ACK messages.<br>• Disable: A DHCP relay agent is disabled from forwarding all DHCP ACK messages.<br>To configure this item, run the **dhcp relay reply forward all enable** command. |
| 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.<br>To specify the parameter, run the **dhcp relay server-select** command. |
| 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.<br>To specify the parameter, run the **dhcp-server** command. |
| VPN instance [xx] | VPN instance bound to the interface. The value xx indicates the index of the VPN instance.<br>**NOTE**<br>This field is displayed in the command output only when a VPN instance is specified using the **dhcp relay server-ip** command. |
| Gateway address in use | IP address of the DHCP gateway.<br>To specify the parameter, run the **gateway** command in the DHCP server group view. |

| Item | Description |
| --- | --- |
| Anycast gateway re-route | Whether the re-routing function for the DHCP relay agent is enabled. The value can be:<br>• Enable: The re-routing function for the DHCP relay agent is enabled.<br>• Disable: The re-routing function for the DHCP relay agent is disabled.<br>To configure this item, run the **dhcp relay anycast gateway re-route enable** command. |
| GIADDR source interface | Source interface of DHCP relayed packets.<br>To configure this item, run the **dhcp relay giaddr source-interface** command. |
| Link-selection insert | Whether the function of inserting the Link-selection suboption of the Option82 field into DHCP packets is enabled. The value can be:<br>• Enable: The function of inserting the Link-selection suboption of the Option82 field into DHCP packets is enabled.<br>• Disable: The function of inserting the Link-selection suboption of the Option82 field into DHCP packets is disabled.<br>To configure this item, run the **dhcp relay information link-selection insert enable** command. |
| Gateway switch | Whether automatic gateway switchover is enabled on a DHCP relay agent. The value can be:<br>• Enable: The automatic gateway switchover on a DHCP relay agent is enabled.<br>• Disable: The automatic gateway switchover on a DHCP relay agent is disabled.<br>To configure this item, run the **dhcp relay gateway-switch enable** command. |

# 6.3.74 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.<br>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

## Usage Guidelines

**Usage Scenario**

You can run the **display dhcp relay statistics** command to view the statistics about the packets received and sent by a DHCP relay agent, so as 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 6-23** 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. |
| 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. |

| Item | Description |
| --- | --- |
| DHCP Bad packets received | DHCP error messages received. |

# 6.3.75 display dhcp server configuration

## Function

The **display dhcp server configuration** command displays DHCP server configuration.

## Format

**display dhcp server configuration**

## Parameters

None

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

When the Switch functions as a DHCP server, you can run the **display dhcp server configuration** command to check DHCP server configuration.

## Example

# Display DHCP server configuration.

```
<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 6-24** Description of the **display dhcp server configuration** command output

| Item | Description |
| --- | --- |
| DHCP server global running information | Global DHCP server configuration. |
| DHCP server bootp | Whether the DHCP server is enabled to respond to BOOTP requests. To configure this item, run the **dhcp server bootp** command. |
| DHCP server bootp automatic | Whether the DHCP server is enabled to dynamically assign IP addresses to BOOTP clients. To configure this item, run the **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 **dhcp server ping** command. |
| DHCP server ping timeout | Maximum time to wait for a response to the ping packet sent by the DHCP server. To configure this item, run the **dhcp server ping** command. |
| DHCP server trust option82 | Whether the DHCP server is enabled to trust the Option 82 field. To configure this item, run the **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 **dhcp server force response** command. |
| DHCP server running information for interface *ifn* | DHCP server configuration on an interface. |
| DHCP server mode | DHCP server mode. The value can be:<br>• Interface: indicates a DHCP server based on an interface address pool. To configure this item, run the **dhcp select interface** command.<br>• Global: indicates a DHCP server based on the global address pool. To configure this item, run the **dhcp select global** command. |

# 6.3.76 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

## 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 6-25** Description of the **display dhcp server database** command output

| Item | Description |
| --- | --- |
| Status | Whether to save the data to the storage device:<br>• disable<br>• enable<br>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:<br>• disable<br>• enable<br>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. |
| 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.<br>The value is set using the **dhcp server database** command. |

# 6.3.77 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

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

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
         VPN instance : vpn1
    Gateway           : 10.10.10.1
```

**Table 6-26** Description of the **display dhcp server group** command output

| Item | Description |
| --- | --- |
| Group-name | Name of a DHCP server group.<br>To specify the parameter, run the **dhcp server group** command. |
| (x) Server-IP | IP addresses of DHCP servers in a DHCP server group. x is the index of the IP addresses and ranges from 0 to 19.<br>To specify the parameter, run the **dhcp-server** command. |
| VPN instance | VPN instance to which the DHCP server group belongs.<br>**NOTE**<br>This field is displayed in the command output only when a VPN instance is specified using the **dhcp-server** command. |

| Item | Description |
| --- | --- |
| Gateway | Gateway address of the DHCP server in the DHCP server group.<br>To specify the parameter, run the **gateway** command in the DHCP server group view. |

# 6.3.78 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

## 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 6-27** 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. |

# 6.3.79 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 6-28** 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. |
| 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. |

| Item | Description |
| --- | --- |
| Rx buffers full or L2fdb lookup failed | Information displayed when the DHCP service is abnormal. The displayed information includes:<br>• Rx buffers full: Total number of DHCP packets discarded because the remaining queue length is shorter than the reserved threshold.<br>• L2fdb lookup failed: Total number of DHCP ACK packets discarded because the DHCP snooping module fails to find user-side interfaces.<br>• High cpu occupancy: Total number of DHCP packets discarded because the CPU usage is excessively high.<br>• Port blocked: Total number of DHCP packets discarded because the inbound interface is blocked.<br>• Bad vlan id: Total number of DHCP packets discarded because the interfaces receiving the DHCP packets are not added to the VLANs corresponding to the VLAN tags carried in the packets or the DHCP packets received on interfaces carry VLAN tags not in the range from 1 to 4094.<br>• Memory exhausted: Total number of DHCP packets discarded because the memory is exhausted.<br>• L3if protocol down: Total number of DHCP packets discarded because the Layer 3 protocol of the source interface goes Down.<br>• Rate limit: Total number of DHCP packets discarded because rates of the packets exceed the limit, when the **dhcp snooping check dhcp-rate enable** command is configured.<br>• Bad packet length: Total number of DHCP packets discarded because the packet length is not in the range of 50 to 2048 bytes.<br>• Bad ip header length: Total number of DHCP packets discarded because the IP header length is not in the range of 20 to 60 bytes |

| Item | Description |
| --- | --- |
| | • Bad ip header checksum: Total number of DHCP packets discarded because the checksum of the IP header is incorrect.<br>• Bad udp checksum: Total number of DHCP packets discarded because the checksum of the UDP header is incorrect.<br>• Hops exceeded: Total number of DHCP request packets discarded by the DHCP relay agent because the hop count exceeds 16.<br>• Bad magic cookie: Total number of DHCP packets discarded because the magic-cookie field is incorrect.<br>• Duplicate option: Total number of DHCP packets discarded because the option fields are duplicate.<br>• Bad option length: Total number of DHCP packets discarded because the option field length is incorrect.<br>• End option absent: Total number of DHCP packets discarded because of the incorrect end option.<br>• Dest-port equals source: Total number of DHCP packets discarded because the source interface is also the outbound interface.<br>• Bad chaddr: Total number of DHCP packets discarded due to incorrect client MAC addresses. A DHCP packet is discarded due to an incorrect client MAC address if a DHCP relay agent finds that the MAC address in the CHADDR field of the DHCP packet is not a unicast address, a DHCP snooping-enabled device finds that the MAC address in the CHADDR field of the DHCP request packet is different from the source MAC address, or the MAC address in the CHADDR field of the DHCP packet conflicts with the DHCP server MAC address.<br>• Bad giaddr: Total number of DHCP packets discarded due to incorrect values in the GIADDR field, when |

| Item | Description |
| --- | --- |
| | the **dhcp snooping check dhcp-giaddr enable** command is configured to check whether the GIADDR field in received DHCP packets is 0 or carries an invalid IP address, such as a loopback address.<br>• Bad request: Total number of invalid DHCP request packets that are discarded, when the **dhcp snooping check dhcp-request enable** command is configured to check the validity of DHCP packets.<br>• Bad reply: Total number of DHCP response packets discarded by untrusted interfaces configured with the **dhcp snooping enable** command.<br>• Bad dest udp-port: Total number of DHCP request packets discarded by the DHCP relay agent because the destination port number is UDP port 68.<br>• Bad message type: Total number of DHCP packets discarded because they are neither requests nor responses.<br>• Max-user limit: Total number of DHCP packets discarded because the maximum number of users (configured by using the **dhcp snooping max-user-number** command) is exceeded.<br>• Add bindtable failed: Total number of DHCP packets discarded because dynamic binding entries are added. New dynamic binding entries may be added if the user-side interface is Down, or IPSG is configured but ACL resources are insufficient.<br>• Client transferred: Total number of DHCP packets discarded because the **undo dhcp snooping user-transfer enable** command is configured to disable location transition for DHCP snooping users. |

| Item | Description |
| --- | --- |
| | • Other error: Total number of DHCP packets discarded due to other reasons. |

# 6.3.80 display ip pool

## Function

The **display ip pool** command displays configured IP address pool information.

## 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** | **l2tp** | **ipsec** | **ssl-vpn** } ] ]

**display ip pool vpn-instance** *vpn-instance-name*

**display ip pool global interface** *interface-type interface-number*

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **interface** *interface-pool-name* | Displays the configuration of the specified interface address pool.<br>**NOTE**<br>An interface address pool is often specified using the interface type and interface number, which are not separated by spaces. | 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 an IP address pool.<br>If *end-ip-address* is specified, the end IP address is also specified. | The value is in dotted decimal notation. |

| Parameter | Description | Value |
| --- | --- | --- |
| **all** | Displays information about all IP addresses in an IP address pool. | - |
| **conflict** | Displays information about conflicting IP addresses in an address pool. (If an IP address that the DHCP server prepares to assign 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 information about expired and idle IP addresses in an IP address pool. | - |
| **used** [ **user-type** { **dhcp** \| **l2tp** \| **ipsec** \| **ssl-vpn** } ] | Displays information about used IP addresses of the specified user type in an IP address pool:<br>• **dhcp** indicates users who obtain IP addresses through DHCP.<br>• **l2tp** indicates L2TP users.<br>• **ipsec** indicates IPSec users.<br>• **ssl-vpn** indicates SSL VPN users. | - |
| **vpn-instance** *vpn-instance-name* | Displays information about the address pool in a specified VPN instance. | The value must be an existing VPN instance name. |
| **global interface** *interface-type interface-number* | Displays information about the address pool on a specified interface.<br>• *interface-type* specifies the interface type.<br>• *interface-number* specifies the interface number. | - |

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

You can run the **display ip pool** command to view information about configured IP address pools and IP addresses in them, including the IP address pool name, lease, lock status, and IP address status.

## Example

# Display information about conflicting addresses in the IP address pool named **test**.

```
<HUAWEI> display ip pool name test conflict
  Pool-name        : test
  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
--------------------------------------------------------------------------------
  Index            IP            Client-ID    Type       Left   Status
--------------------------------------------------------------------------------
    109   192.168.0.110                  -       -          -   Conflict
--------------------------------------------------------------------------------
```

**Table 6-29** Description of the **display ip pool** command output

| Item | Description |
| --- | --- |
| Pool-name | Name of an IP address pool.<br>To configure this parameter, run the **ip pool (system view)** command. |
| Pool-No | Index of the IP address pool. |

| Item | Description |
| --- | --- |
| Lease | Lease of the IP address pool.<br>To configure this parameter, run the **lease** command. |
| Domain-name | Domain name.<br>To configure this parameter, run the **domain-name** command. |
| Option-code | Value of a customized option.<br>To configure this parameter, run the **option** command. |
| Option-subcode | Value of a customized sub-option.<br>To configure this parameter, run the **option** command. |
| Option-type | Type of a customized option code:<br>● ascii: indicates that the customized option code is an ASCII character string.<br>● hex: indicates that the customized option code is a hexadecimal string.<br>● cipher: indicates that the customized option code is a ciphertext character string.<br>To configure this parameter, run the **option** command. |
| Option-value | Content of a customized option.<br>To configure this parameter, run the **option** command. |
| 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.<br>To configure this parameter, 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.<br>To configure this parameter, run the **nbns-list** command. |

| Item | Description |
| --- | --- |
| Netbios-type | NetBIOS type.<br>To configure this parameter, run the **netbios-type** command. |
| Position | Position of the IP address pool. |
| Status (First) | Status of the IP address pool.<br>To configure this parameter, 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.<br>To configure this parameter, run the **gateway-list** command. |
| Network | Network segment of the IP address pool. |
| Mask | Subnet mask of the IP address pool.<br>To configure this parameter, run the **network (IP address pool view)** command. |
| Bootfile | Name of the startup configuration file configured for the DHCP client.<br>To configure this parameter, run the **bootfile** command. |
| VPN instance | Name of a VPN instance. |
| Logging | Status of the logging function when the DHCP server assigns IP addresses.<br>• Enable<br>• Disable<br>To configure this parameter, run the **logging** or **dhcp server logging** command. |
| Conflicted address recycle interval | Interval for automatically reclaiming conflicting IP addresses in the IP address pool.<br>To configure this parameter, run the **conflict auto-recycle interval day** *day* [ **hour** *hour* [ **minute** *minute* ] ] command. |

| Item | Description |
| --- | --- |
| Address Statistic | Statistics about IP addresses in the IP 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 IP address pool.<br>Total = Used + Idle(Expired) + Conflict + Disable |
| Used | Number of used IP addresses in the IP address pool. |
| Idle(Expired) | Number of idle (expired) IP addresses in the address pool.<br>**NOTE**<br>If the mask length of the address pool is shorter than that of the interface IP address on the DHCP server, users may fail to go online even when there are idle IP addresses in the address pool. |
| Conflict | Number of conflicting IP addresses in the IP address pool.<br>**NOTE**<br>If there are many conflicting IP addresses in the address pool, it is recommended that you configure the **conflict auto-recycle interval** command to reclaim conflicting IP addresses periodically. This configuration reduces occupation of idle IP addresses in the address pool and prevents IP address conflicts on the network. |
| Disabled | Number of disabled IP addresses in the IP address pool. |

| Item | Description |
| --- | --- |
| Client-ID format as follows | Client ID format:<br>• DHCP: mac-address. The client ID format of DHCP users is a MAC address.<br>• PPPoE: mac-address. The client ID format of PPPoE users is a MAC address.<br>• IPSec: user-id/portnumber/vrf. The client ID format of IPSec users is a user ID, port number, or VPN index.<br>• PPP: interface index. The client ID format of PPP users is an interface index.<br>• L2TP: cpu-slot/session-id. The client ID format of L2TP users is a CPU ID-slot ID or session ID.<br>• 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.<br>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**. |

| Item | Description |
| --- | --- |
| Status (Second) | Status of an IP address:<br>• Used: indicates that the IP address is used.<br>• Idle: indicates that the IP address is idle.<br>• Expired: indicates that the lease of the IP address expires and the IP address is idle.<br>• Conflict: indicates that the IP address conflicts with another IP address on the network.<br>• Disable: indicates that the IP address cannot be used.<br>• Static-bind: indicates that the IP address is bound to a MAC address.<br>• Static-bind used: indicates that the IP address is bound to a MAC address and used. |

# 6.3.81 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. | - |
| **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
```

# 6.3.82 domain-name

## Function

The **domain-name** command configures the domain name suffix for DHCP clients.

The **undo domain-name** command deletes a configured domain name suffix.

By default, no domain name suffix is configured for DHCP clients.

## 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.<br>**NOTE**<br>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 an IP address to a client, a DHCP server can also assign a domain name suffix to the client. You can run the **domain-name** command on the DHCP server to specify the domain name suffix for clients. After this command is run, the DHCP server will send the domain name suffix to a client when allocating an IP addresses to the client.

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**.

```
<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 **example.com**.

```
<HUAWEI> system-view
[HUAWEI] dhcp option template template1
[HUAWEI-dhcp-option-template-template1] domain-name example.com
```

# 6.3.83 excluded-ip-address

## Function

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

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

By default, all IP addresses in an 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 of the IP address segment where addresses cannot be automatically assigned to clients. | The value is in dotted decimal notation. |
| *end-ip-address* | Specifies the end IP address of the IP address segment where addresses cannot be automatically assigned to clients. If *end-ip-address* is not specified, only the IP address corresponding to *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

## 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 such IP address conflicts, you need to exclude these IP addresses from being automatically assigned 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 (IP 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 **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 status of the interface IP address to Conflict during address assignment.
- If you run the **excluded-ip-address** command multiple times, you can specify multiple IP addresses or ranges of IP addresses that cannot be automatically assigned to clients from the specified address pool.
- You can run the **display ip pool** command to check the IP addresses in use in the current address pool, so that you can exclude the unused IP addresses from being automatically assigned to clients. If you need to exclude IP addresses in Used and Conflict states from being automatically assigned to clients after address reclamation, you can also run the **excluded-ip-address** command. If an IP address has been bound to a specific MAC address, adding the IP address to the IP address list in which IP addresses are not

automatically assigned to clients will unbind the IP address from the MAC address.

## Example

# Disable IP addresses 10.10.10.10 to 10.10.10.20 from being automatically assigned to clients from the address pool **global1**.

```
<HUAWEI> system-view
[HUAWEI] ip pool global1
[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
```

# Disable IP address 10.10.10.30 in Used state from being automatically assigned to clients from the address pool **global1**.

```
<HUAWEI> system-view
[HUAWEI] ip pool global1
[HUAWEI-ip-pool-global1] network 10.10.10.0 mask 24
[HUAWEI-ip-pool-global1] excluded-ip-address 10.10.10.30
Warning: The address is in used or conflict state. Are you sure to continue excluding the address?[Y/N]:y
```

# 6.3.84 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**

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
```

# 6.3.85 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**

## 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 VLANIF interface address as the gateway address to communicate with the DHCP server.
- When two switch 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
```

# 6.3.86 gateway-list

## Function

The **gateway-list** command configures an egress gateway address for a DHCP client.

The **undo gateway-list** command deletes a configured egress gateway address.

By default, no egress gateway address is configured.

## Format

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

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

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *ip-address* | Specifies the IP address of an egress gateway. | 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.

To configure an egress gateway for a DHCP relay agent, run the **gateway (DHCP server group view)** command.

**Configuration Impact**

If a gateway address is configured on the DHCP server, a DHCP client will obtain 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**

- The IP addresses specified in the **excluded-ip-address** command cannot be configured as a gateway address.
- After an IP address is configured as a gateway address, the device adds the IP address to the list of IP addresses that cannot be automatically allocated, removing the need to run the **excluded-ip-address** command.
- In the IP address pool view or DHCP Option template view, a maximum of eight egress gateway addresses can be configured on the device. These gateway addresses cannot be subnet broadcast addresses.
- When configuring an egress gateway address for the global address pool of a DHCP server, ensure that this egress gateway address is the same as that of the DHCP relay agent.

## 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 view, 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
```

# 6.3.87 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

| Parameter | Description | Value |
| --- | --- | --- |
| **unicast** | Indicates that the client requests the server to unicast response packets to the client. | - |

## Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

## 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 Switch 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 VLANIF100 to obtain an IP address.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address bootp-alloc
```

# Enable the BOOTP client function on GE0/0/1 to obtain an IP address.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address bootp-alloc
```

# 6.3.88 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 enabled on VLANIF 1 of the S1720GW-E and S1720GWR-E. On other devices, the DHCP client function is disabled on an interface.

## 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

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

To enable an interface on the Switch to obtain an IP address using DHCP, enable the DHCP client function on the interface. A DHCP client applies for an IP address from the server using DHCP. The DHCP client has two functions:

- Sends DHCPREQUEST messages to the server.
- Processes DHCPACK messages from the server.

To obtain an IP address, the DHCP client sends a DHCPREQUEST message to the server. After the server receives the DHCPREQUEST message, it sends a DHCPACK message to the DHCP client. The DHCP client obtains the assigned IP address from the DHCPACK 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 configuration. If no IP address is obtained through the **ip address dhcp-alloc** command, running the **undo ip address** command does not delete the **ip address dhcp-alloc** command configuration.

For the S1720GW-E and S1720GWR-E, if no IP address is configured on the device, VLANIF 1 uses the IP address 192.168.1.253 255.255.255.0 by default, and the **ip address dhcp-alloc unicast** command is configured on the interface by default. After VLANIF 1 obtains an IP address through DHCP successfully, the IP address 192.168.1.253 255.255.255.0 is deleted. If the DHCP client function is enabled on another VLANIF interface, the VLANIF interface cannot obtain the IP address in the same network segment as that of VLANIF 1, which prevents address conflict.

## Example

# Enable the DHCP client function on VLANIF100 to obtain an IP address.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address dhcp-alloc
```

# Enable the DHCP client function on GE0/0/1 to obtain an IP address.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip address dhcp-alloc
```

# 6.3.89 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 case-insensitive 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** 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.

**Precautions**

A maximum of 128 address pools, including global address pools and interface address pools, can be created on the device.

**Follow-up Procedure**

Run the **network** command in the IP address pool view to specify the range of the IP addresses that can be allocated in the pool.

## Example

# Create a global address pool named **global1**.

```
<HUAWEI> system-view
[HUAWEI] ip pool global1
```

# 6.3.90 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

## 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.

**Precautions**

After the **ip relay address cycle** command is run, the DHCP relay agent forwards a received DHCP Discover message to a different DHCP server each time in the sequence in which DHCP servers were configured. You can run the **display dhcp relay** command to view DHCP server IP addresses in the **Server IP address** field to determine the sequence in which DHCP servers were configured.

## Example

# Enable DHCP server polling on the switch in the system view.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] ip relay address cycle
```

# 6.3.91 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* ]

## 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. |

| Parameter | Description | Value |
| --- | --- | --- |
| *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 VLANIF100 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 vlanif 100 dhcp 30
```

# 6.3.92 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** 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 **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 **ip pool** 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
```

# 6.3.93 lock (IP address pool view)

## Function

The **lock** command locks an IP address pool.

The **undo lock** restores the default configuration.

By default, no IP address pool is locked.

## Format

**lock**

**undo lock**

## Parameters

None

## Views

IP address pool view

## Default Level

2: Configuration level

## Usage Guidelines

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.

## Example

# Lock the IP address pool **global1**.

```
<HUAWEI> system-view
[HUAWEI] ip pool global1
[HUAWEI-ip-pool-global1] lock
```

# 6.3.94 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.

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**

- 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 in the *CLI-based Configuration - Device Management Configuration Guide*.

  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
```

# 6.3.95 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. |
| **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
```

# 6.3.96 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

## 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
```

# 6.3.97 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, the range of IP addresses that can be dynamically allocated is not configured.

## Format

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

**undo network**

## 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. | 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 to 7, 31, or 32.
- If you need to assign IP addresses with a 16-bit mask in the network segment 10.1.1.0 to clients, the number of IP addresses in an IP address pool is 64K after the **network 10.1.1.0 mask 16** command is executed in the view of the IP address pool. If the number of IP addresses in the IP address pool is less than 64K, the **network 10.1.1.0 mask 16** command cannot be executed in the view of the IP address pool. In this case, perform the following operations:

  Run the following commands in the IP address pool view:

  ```
  [HUAWEI-ip-pool-test] ip pool test
  [HUAWEI-ip-pool-test] section 0 10.1.1.2 10.1.1.254  // The section command specifies the range of IP addresses to be allocated.
  [HUAWEI-ip-pool-test] network 10.1.1.1 mask 16  // The network command specifies the mask of IP addresses to be allocated using the mask parameter.
  ```

  Enable the DHCP server function on a specific interface.

  ```
  [HUAWEI-Vlanif10] ip address 10.1.1.1 16
  [HUAWEI-Vlanif10] dhcp select global
  ```

- The size of the IP address pool cannot be larger than 16K.

## 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
```

# 6.3.98 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, 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
```

# 6.3.99 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* ] ]

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *code* | Specifies the code of a user-defined option. | The value is an integer that ranges from 1 to 254, except the values 1, 3, 6, 15, 44, 46, 50, 51, 52, 53, 54, 55, 57, 58, 59, 61, 82, 120, 121, and 184.<br>**NOTE**<br>There are well-known options and user-defined options. For details about well-known options, see RFC 2132.<br>When the switch functions as a DHCP client, Option 148 can be used in an EasyDeploy scenario and is not recommended in other scenarios. |
| **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 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. |

| Parameter | Description | Value |
| --- | --- | --- |
| **hex** *hex-string* | Specifies the user-defined option code as a hexadecimal character 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 characters; if **sub-option** is specified, the value without spaces ranges from 1 to 252. The value can be a combination of digits (0-9), uppercase letters (A-F), and lowercase letters (a-f). |
| **cipher** *cipher-string* | Specifies the user-defined option code as a ciphertext character string. | The value is a character string either in plain text or cipher text.<br>• The character string in plain text is a string of 1 to 64 characters.<br>• The character string in cipher text is a string of 32 to 108 characters.<br>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 configuration accuracy, read the Request For Comments (RFC) before configuring options.
- When an option contains a password, the option code of the **ascii** or **hex** type is insecure. You are advised to set the option code type to **cipher**. For security purposes, a password must contain at least two types of the following: lowercase letters, uppercase letters, digits, and special characters. In addition, the password must consist of at least eight 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 the 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.
- If the device functions as the DHCP server to assign IP addresses to APs, and the AC and APs are on different network segments, you need to configure the Option 43 field to specify the AC IP address for the APs. Otherwise, the APs cannot discover the AC. Run the **option 43** { **hex** *hex-string* | [ **sub-option** 1 **hex** *hex-string* | **sub-option** 2 **ip-address** *ip-address* &<1-8> | **sub-option** 3 **ascii** *ascii-string* ] } command to configure the device to specify the AC IP address for APs in one of the following methods:
  a. Run the **option 43 hex 031D3139322e3136382e3139342e35302c3139322e3136382e3139342e3534** command to configure the device to specify AC IP addresses 192.168.194.50 and 192.168.194.54 for APs. In this command, **03** indicates that the sub-option value of Option43 is an ASCII value; **1D** indicates that the length of IP addresses (192.168.194.50,192.168.194.54) including dots (.) and the comma (,) is 29, and multiple IP addresses are separated by the comma (,); **3139322e3136382e3139342e3530** indicates the ASCII value of 192.168.194.50; **2C** indicates the ASCII value of the

comma (,); **3139322e3136382e3139342e3534** indicates the ASCII value of 192.168.194.54.

b. Run the **option 43 sub-option 1 hex C0A80001C0A80002** command to configure the device to specify AC IP addresses 192.168.0.1 and 192.168.0.2 for APs. In the command, **C0A80001** indicates the hexadecimal format of 192.168.0.1, and **C0A80002** indicates the hexadecimal format of 192.168.0.2.

c. Run the **option 43 sub-option 2 ip-address 192.168.0.1 192.168.0.2** command to configure the device to specify AC IP addresses 192.168.0.1 and 192.168.0.2 for APs.

d. Run the **option 43 sub-option 3 ascii 192.168.0.1,192.168.0.2** command to configure the device to specify AC IP addresses 192.168.0.1 and 192.168.0.2 for APs.

NOTE

If you need to configure multiple IP addresses when the option is specified as an ASCII character string, use commas (,) to separate the IP addresses.

If the AC and APs are on the same network segment, you do not need to configure the Option 43 field, and the APs can discover the AC in broadcast mode. After Option 43 is configured, the APs unicast Discover Request packets to the IP address carried in Option 43 to discover the AC. If the APs do not receive any Discovery Response packet after sending unicast Discovery Request packets, the APs then broadcast packets to discover the AC.

- When users on an enterprise's intranet use a proxy server to connect to the Internet, you need to configure proxy server parameters so that users can use browsers to access the network. The Web Proxy Auto-Discovery Protocol (WPAD) implements automatic configuration of these parameters. The administrator does not need to manually configure these parameters on each client. To implement the WPAD function, the administrator needs to deploy the configuration file of the proxy server in advance, and then run the **option 252 ascii** *ascii-string* command to specify the URL of the configuration file. The *ascii-string* parameter specifies the URL of the configuration file, in the format of https://*xxx*/proxy.pac. Set *ascii-string* according to the storage path of the configuration file. When a browser accesses the network, the browser requests the DHCP server to send the URL of the configuration file on the proxy server, and then downloads the configuration file to conduct automatic configuration. After the configuration is completed, the browser can access the network.

  NOTE

  The value of *ascii-string* cannot be enclosed in double quotation marks as "*ascii-string*". Otherwise, terminals cannot parse Option252.

## 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
```

# 6.3.100 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* ]

## 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
```

# 6.3.101 option125 vendor-specific

## Function

The **option125 vendor-specific** command configures the vendor ID in Option 125 for a DHCP client.

The **undo option125 vendor-specific** command deletes the vendor ID in Option 125 for a DHCP client.

By default, no vendor ID is configured in Option 125.

## Format

**option125 vendor-specific** *vendor-id*

**undo option125 vendor-specific**

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *vendor-id* | Indicates the vendor ID, which is assigned by the IANA. 2011 indicates Huawei. | The value is an integer in the range from 1 to 4294967295. |

## Views

IP address pool view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

If a DHCP client sends a DHCP Discover message carrying a vendor ID to a DHCP server, the DHCP server needs to exchange the vendor information with the client using Option 125. You can run the **option 125** [ **sub-option** *sub-code* ] **ascii** *ascii-string* command to configure the vendor ID in Option 125 delivered by a DHCP server to a client. However, it is complex to convert the vendor ID into an ASCII character string.

To simplify the configuration, you can run the **option125 vendor-specific** *vendor-id* command to specify the vendor ID in Option 125 of packets sent from a DHCP server to a client.

**Prerequisites**

1. A global address pool has been created using the **ip pool** command in the system view, and the IP address pool view is displayed.
2. Fields except **Vendor-ID** in Option 125 have been configured for the global address pool using the **option 125 ascii** *ascii-string* command. The **Vendor-ID** field in Option 125 occupies four bytes. Therefore, the *ascii-string* value is a string of 1 to 251 bytes.
3. (Optional) The **force insert option 125** command has been used to configure the DHCP server to insert the Option 125 field specified for the global address pool into the DHCP response packet sent from a DHCP server to a client. This resolves the problem in the following situation: The device functions as a DHCP server, and the DHCP request packet sent by a DHCP client does not carry Option 125. However, the DHCP client still expects the DHCP server to deliver Option 125 configured for the global address pool.

**Precautions**

This command and the **option 125 sub-option** *sub-code* **ascii** *ascii-string* command are mutually exclusive in an IP address pool.

## Example

# Configure the VLAN and vendor information in Option 125 in the IP address pool view.

```
<HUAWEI> system-view
[HUAWEI] ip pool global1
[HUAWEI-ip-pool-global1] option 125 ascii id:vlan=10
[HUAWEI-ip-pool-global1] option125 vendor-specific 2011
```

# 6.3.102 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** ]

## 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

## 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
```

# 6.3.103 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.<br>• *interface-type* specifies the interface type.<br>• *interface-number* specifies the interface number. | - |

## 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**

# 6.3.104 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* ]

## 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
```

# 6.3.105 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
```

# 6.3.106 reset dhcp statistics

## Function

The **reset dhcp statistics** command clears packet statistics about a DHCP.

## 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
```

# 6.3.107 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** }

## 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**

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.

User information cannot be restored after you clear it. Exercise caution when running the **reset ip pool** command. DHCP clients must release their old IP addresses before obtaining new IP addresses.

**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
```

# 6.3.108 section (IP address pool view)

## Function

The **section** command configures an IP address range in an IP address pool.

The **undo section** command deletes a configured IP address range from an IP address pool.

By default, no IP address range is configured in an IP address pool.

## Format

**section** *section-id start-address* [ *end-address* ]

**undo section** *section-id*

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *section-id* | Specifies the ID of an address range in an IP address pool. | The value is an integer in the range from 0 to 255. |

| Parameter | Description | Value |
| --- | --- | --- |
| *start-address* | Specifies the start IP address of the address range. | The value is in dotted decimal notation. |
| *end-address* | Specifies the end IP address of the address range.<br>**NOTE**<br>The end IP address must be greater than or equal to the start IP address. If the end IP address is not specified, the IP address range contains only one IP address. | 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 ranges. The IP addresses in the IP address ranges cannot overlap.

## Example

# Configure an IP address range 10.1.1.10 to 10.1.1.15 in the IP address pool **abc**, and set the ID of the IP address range to 0.

```
<HUAWEI> system-view
[HUAWEI] ip pool abc
[HUAWEI-ip-pool-abc] section 0 10.1.1.10 10.1.1.15
```

# 6.3.109 sip-server (IP address pool view)

## 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.

## 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
```

# 6.3.110 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. When double 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

### 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.

### 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 **example**.

```
<HUAWEI> system-view
[HUAWEI] dhcp option template template1
[HUAWEI-dhcp-option-template-template1] sname example
```

# 6.3.111 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.

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 1 to 4 digits. |

| Parameter | Description | Value |
| --- | --- | --- |
| **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

## 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 **excluded-ip-address** command.
- 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. 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 192.168.1.10 in the global address pool **global1** to a host with the MAC address 00e0-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 00e0-fc96-e4c0
```

# 6.3.112 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 name. |

## 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 **example**.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance example
[HUAWEI-vpn-instance-example] ipv4-family
[HUAWEI-vpn-instance-example-af-ipv4] quit
[HUAWEI-vpn-instance-example] quit
[HUAWEI] ip pool global1
[HUAWEI-ip-pool-global1] vpn-instance example
```

# 6.4 DHCP Policy VLAN Configuration Commands

## 6.4.1 Command Support

Only the following switch models support DHCP policy VLAN:

S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S

# 6.4.2 dhcp policy-vlan generic

## Function

The **dhcp policy-vlan generic** command configures the generic DHCP policy VLAN.

The **undo dhcp policy-vlan generic** command deletes the generic DHCP policy VLAN.

By default, the function of generic DHCP policy VLAN is disabled on the device.

## Format

**dhcp policy-vlan generic** [ **priority** *priority* ]

**undo dhcp policy-vlan generic**

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **priority** *priority* | Specifies the 802.1p priority of DHCP messages. | The value is an integer that ranges from 0 to 7. The default value is 0. |

## Views

VLAN view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

You can configure three types of DHCP policy VLAN on the device at the same time. They are listed in descending order based on priorities as follows:

- DHCP policy VLAN based on MAC addresses
- DHCP policy VLAN based on interfaces
- Generic DHCP policy VLAN

On a network supporting VLAN assignment based on IP subnets, upon receiving an untagged packet from a host, a switch adds a VLAN ID to the packet based on the source IP address of the packet. A host that accesses the network for the first time does not have a valid IP address. Therefore, the switch cannot add the host to the VLAN and the host cannot obtain a valid IP address or network settings. To make the host obtain a valid IP address from the DHCP server, run the **dhcp policy-vlan generic** command to configure the generic policy VLAN.

Hosts that access the network for the first time apply the generic DHCP policy VLAN only when they cannot apply DHCP policy VLAN based on MAC addresses or interfaces.

**Prerequisites**

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

**Precautions**

If you run this command in multiple VLAN views, only the latest configuration takes effect.

## Example

# Configure the generic DHCP policy VLAN, associate DHCP packets that match no MAC address or interface to VLAN 100, and set the 802.1p priority of the packets to 5.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] dhcp policy-vlan generic priority 5
```

# 6.4.3 dhcp policy-vlan mac-address

## Function

The **dhcp policy-vlan mac-address** command configures the MAC address-based DHCP policy VLAN.

The **undo dhcp policy-vlan mac-address** command deletes the MAC address-based DHCP policy VLAN.

By default, the function of DHCP policy VLAN based on MAC addresses is disabled on the device.

## Format

**dhcp policy-vlan mac-address** *mac-address1* [ **to** *mac-address2* ] [ **priority** *priority* ]

**undo dhcp policy-vlan mac-address** *mac-address1* [ **to** *mac-address2* ]

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *mac-address1* [ **to** *mac-address2* ] | Specifies the MAC addresses of user hosts that access the network for the first time.<br>• *mac-address1* specifies the start MAC address.<br>• **to** *mac-address2* specifies the end MAC address. *mac-address2* must be greater than *mac-address1*. *mac-address2* and *mac-address1* specify the MAC address range. If **to** *mac-address2* is not specified, DHCP policy VLAN based on only the MAC address specified by *mac-address1* is configured. | *mac-address1* and *mac-address2* are in the format of H-H-H. An H contains one to four hexadecimal numbers.<br>**NOTE**<br>The range specified by *mac-address1* and *mac-address2* cannot contain multicast MAC addresses, broadcast MAC addresses, and all 0 address. The number of MAC addresses cannot exceed 512. |
| **priority** *priority* | Specifies the 802.1p priority of DHCP messages. | The value is an integer that ranges from 0 to 7. The default value is 0. |

## Views

VLAN view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

You can configure three types of DHCP policy VLAN on the device at the same time. They are listed in descending order based on priorities as follows:

- DHCP policy VLAN based on MAC addresses
- DHCP policy VLAN based on interfaces
- Generic DHCP policy VLAN

On a network supporting VLAN assignment based on IP subnets, upon receiving an untagged packet from a host, a switch adds a VLAN ID to the packet based on the source IP address of the packet. A host that accesses the network for the first

time does not have a valid IP address. Therefore, the switch cannot add the host to the VLAN and the host cannot obtain a valid IP address or network settings. To make the host obtain a valid IP address from the DHCP server, run the **dhcp policy-vlan mac-address** command to configure the MAC address-based DHCP policy VLAN.

**Prerequisites**

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

**Precautions**

If you run this command based on the same MAC address in multiple VLAN views, only the latest configuration takes effect.

## Example

# Configure the MAC address-based DHCP policy VLAN, associate DHCP packets from the host with the MAC address 00e0-fc01-0001 to VLAN 100, and set the 802.1p priority of the packets to 5.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] dhcp policy-vlan mac-address 1-1-1 priority 5
```

# 6.4.4 dhcp policy-vlan port

## Function

The **dhcp policy-vlan port** command configures the interface-based DHCP policy VLAN.

The **undo dhcp policy-vlan port** command deletes the interface-based DHCP policy VLAN.

By default, the function of DHCP policy VLAN based on interfaces is disabled on the device.

## Format

**dhcp policy-vlan port** *interface-type interface-number1* [ **to** *interface-number2* ] &<1-10> [ **priority** *priority* ]

**undo dhcp policy-vlan port** *interface-type interface-number1* [ **to** *interface-number2* ] &<1-10>

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *interface-type interface-number1* [ **to** *interface-number2* ] &<1-10> | Specifies the interface type and interface number.<br>• *interface-type* specifies the type of an interface.<br>• *interface-number1* specifies the number of the start interface.<br>• **to** *interface-number2* specifies the number of the end interface. *interface-number2*must be greater than *interface-number1*. *interface-number2* and *interface-number1* specify the interface range. If **to** *interface-number2* is not specified, DHCP policy VLAN based on only the interface specified by *interface-number1* is configured.<br>**NOTE**<br>The interface cannot be a stack interface. | - |
| **priority** *priority* | Specifies the 802.1p priority of DHCP messages. | The value is an integer that ranges from 0 to 7. The default value is 0. |

## Views

VLAN view

## Default Level

2: Configuration level

## Usage Guidelines

### Usage Scenario

You can configure three types of DHCP policy VLAN on the device at the same time. They are listed in descending order based on priorities as follows:

- DHCP policy VLAN based on MAC addresses

- DHCP policy VLAN based on interfaces
- Generic DHCP policy VLAN

On a network supporting VLAN assignment based on IP subnets, upon receiving an untagged packet from a host, a switch adds a VLAN ID to the packet based on the source IP address of the packet. A host that accesses the network for the first time does not have a valid IP address. Therefore, the switch cannot add the host to the VLAN and the host cannot obtain a valid IP address or network settings. To make the host obtain a valid IP address from the DHCP server, run the **dhcp policy-vlan port** command to configure the interface-based policy VLAN.

**Prerequisites**

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

**Precautions**

If you run this command on an interface in multiple VLAN views, only the latest configuration takes effect.

NOTE

The interface-based DHCP policy VLAN takes effect only for hybrid interfaces. If an interface is not hybrid, run the **port link-type hybrid** command to configure it as a hybrid interface.

### Example

# Configure the interface-based DHCP policy VLAN, associate DHCP packets received on GigabitEthernet0/0/1 with VLAN 100, and set the 802.1p priority of the packets to 5.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI--GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI--GigabitEthernet0/0/1] quit
[HUAWEI] dhcp enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] dhcp policy-vlan port gigabitethernet 0/0/1 priority 5
```

# 6.5 DNS Configuration Commands

## 6.5.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

## 6.5.2 display dns dynamic-host

### Function

The **display dns dynamic-host** command displays dynamic DNS entries.

## Format

**display dns dynamic-host** [ **vpn-instance** *vpn-instance-name* | **all** ]

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **vpn-instance** *vpn-instance-name* | Displays dynamic DNS entries of a specified VPN instance. | The value must be an existing VPN instance name. |
| **all** | Displays all dynamic DNS entries, including both public and private DNS entries.<br>**NOTE**<br>If neither **vpn-instance** *vpn-instance-name* nor **all** is specified, only public dynamic DNS entries are displayed. | - |

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

You can run the **display dns dynamic-host** command to view dynamic DNS entries and check whether domain names match the mapping entries.

## Example

# Display dynamic DNS entries.

```
<HUAWEI> display dns dynamic-host
No  Domain-name       IpAddress     TTL    Alias
1   www.example.com    10.1.1.1     3521
2   www.huawei.com     10.1.2.1     3000
```

# Display dynamic DNS entries of the VPN instance vpn1.

```
<HUAWEI> display dns dynamic-host vpn-instance vpn1
No  Domain-name                Alias              IpAddress        TTL     VPN-Instance
1   www.example.com                               10.1.3.1         3521    vpn1
2   www.huawei.com                                10.1.4.1         3000    vpn1
```

**Table 6-30** Description of the **display dns dynamic-host** command output

| Item | Description |
| --- | --- |
| No | Number of a dynamic DNS entry. |
| Domain-name | Domain name. |
| IpAddress | IP addresses of the host. |
| TTL | Remaining lifetime of DNS entries (in seconds). |
| Alias | Alias of a host. |
| VPN-Instance | VPN instance name. |

## 6.5.3 display dns domain

### Function

The **display dns domain** command displays information about the domain name suffixes.

### Format

**display dns domain** [ **vpn-instance** *vpn-instance-name* | **all** ]

### Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **vpn-instance** *vpn-instance-name* | Displays information about domain name suffixes of a specified VPN instance. | The value must be an existing VPN instance name. |
| **all** | Displays information about all domain name suffixes, including both public and private domain name suffixes.<br>**NOTE**<br>If neither **vpn-instance** *vpn-instance-name* nor **all** is specified, only information about public domain name suffixes is displayed. | - |

### Views

All views

### Default Level

1: Monitoring level

## Usage Guidelines

The **display dns domain** command displays the configuration of domain name suffixes and the order in which they are configured.

## Example

# Display the list of domain name suffixes.

```
<HUAWEI> display dns domain
No                Domain-name
1                 com
2                 net
```

# Display the list of domain name suffixes of the VPN instance vpn1.

```
<HUAWEI> display dns domain vpn-instance vpn1
No          Domain-name          VPN-Instance
1           com.cn               vpn1
```

**Table 6-31** Description of the **display dns domain** command output

| Item | Description |
| --- | --- |
| No | Indicates the domain name suffix numbers, that is, the configuration sequence of domain name suffixes. |
| Domain-name | Indicates the configured domain name suffix. If there are multiple domain name suffixes in the list, during DNS resolution, the first suffix 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 next suffix is added and sent to the DNS server for searching for the mapped address.<br>The value is set using the **dns domain** command. |
| VPN-Instance | VPN instance name.<br>The value is set using the **dns domain** command. |

# 6.5.4 display dns server

## Function

The **display dns server** command displays information about DNS servers.

## Format

**display dns server** [ **vpn-instance** *vpn-instance-name* | **all** ]

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **vpn-instance** *vpn-instance-name* | Displays information about DNS servers of a specified VPN instance. | The value must be an existing VPN instance name. |
| **all** | Displays information about all DNS servers, including both public and private DNS servers.<br>**NOTE**<br>If neither **vpn-instance** *vpn-instance-name* nor **all** is specified, only information about public DNS servers is displayed. | - |

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

After configuring DNS server addresses, you can run the **display dns server** command to view the configuration and sequence of DNS servers.

## Example

# Display information about DNS servers.

```
<HUAWEI> display dns server
IPv4 Dns Servers :
Domain-server       IpAddress
    1               10.16.1.1
    2               10.17.1.1

IPv6 Dns Servers :
Domain-server       Ipv6Address                          (Interface Name)
    1               FC00:1::1
```

# Display information about the DNS servers of the VPN instance vpn1.

```
<HUAWEI> display dns server vpn-instance vpn1
IPv4 Dns Servers :
Domain-server       IpAddress          VPN-Instance
    1               172.16.1.1         vpn1
    2               172.16.1.2         vpn1

IPv6 Dns Servers :
No configured servers.
```

**Table 6-32** Description of the **display dns server** command output

| Item | Description |
| --- | --- |
| IPv4 Dns Servers | IPv4 DNS server configuration. |
| Domain-server | DNS server number, indicating the order in which they were configured. |
| IpAddress | IP address of the DNS server. During DNS resolution, the first DNS server is used. If this server fails to resolve packets, the second DNS server is used.<br>The value is set using the **dns server** command. |
| IPv6 Dns Servers | IPv6 DNS server configuration. |
| Ipv6Address | IPv6 address of the IPv6 DNS server.<br>The value is set using the **dns server ipv6** command. |
| Interface Name | Interface name, which only corresponds to the local IPv6 link address.<br>The value is set using the **dns server ipv6** command. |
| VPN-Instance | VPN instance name.<br>The value is set using the **dns server** command. |

## 6.5.5 display ip host

### Function

The **display ip host** command displays the static DNS entries.

### Format

**display ip host** [ **vpn-instance** *vpn-instance-name* | **all** ]

### Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **vpn-instance** *vpn-instance-name* | Displays static DNS entries of a specified VPN instance. | The value must be an existing VPN instance name. |

| Parameter | Description | Value |
| --- | --- | --- |
| **all** | Displays all static DNS entries, including both public and private static DNS entries.<br>**NOTE**<br>If neither **vpn-instance** *vpn-instance-name* nor **all** is specified, only public static DNS entries are displayed. | - |

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

After running the **ip host** command to configure static DNS entries, you can run this command to check whether mappings between host names and IP addresses are correct. You can run the **display ip host** command to view static DNS entries.

## Example

# Display static DNS entries.

```
<HUAWEI> display ip host
Host                 Age        Flags  Address
www.3322.org         0          static 10.1.1.1
members.3322.org     0          static 10.1.2.1
checkip.dyndns.com   0          static 10.1.3.1
members.dyndns.org   0          static 10.1.4.1
```

# Display static DNS entries of VPN instance vpn1.

```
<HUAWEI> display ip host vpn-instance vpn1
Host          Age         Flags      Address        VPN-Instance
RTB           0           static     10.1.5.1       vpn1
```

**Table 6-33** Description of the **display ip host** command output

| Item | Description |
| --- | --- |
| Host | Host name.<br>The value is set using the **ip host** command. |
| Age | Aging time. The value 0 indicates a static DNS entry. Static entries are not aged out. |
| Flags | Status of the domain name. The value static indicates a static domain name. |

| Item | Description |
| --- | --- |
| Address | IP address mapping the domain name.<br>The value is set using the **ip host** command. |
| VPN-Instance | VPN instance name.<br>The value is set using the **ip host** command. |

## 6.5.6 dns domain

### Function

The **dns domain** command configures a domain name suffix.

The **undo dns domain** command deletes a domain name suffix.

By default, no domain name suffix is configured.

### Format

**dns domain** *domain-name* [ **vpn-instance** *vpn-instance-name* ]

**undo dns domain** [ *domain-name* [ **vpn-instance** *vpn-instance-name* ] ]

### Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *domain-name* | Specifies the suffix of a domain name. | The value is a string of 1 to 63 characters without spaces. A combination of digits, letters, underscores (_), hyphens (-), and dots (.) is allowed. |
| **vpn-instance** *vpn-instance-name* | Specifies the name of a VPN instance. | The value must be an existing VPN instance name. |

### Views

System view

### Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

Many servers or hosts have the same suffix. In this case, you can configure domain name suffixes. For example, you can configure a suffix com.cn for the host whose domain name is huawei. When a DNS client accesses the host, it enters only "huawei" to send a query message to the DNS server. The DNS client automatically adds the suffix com.cn. Then the DNS server searches for the IP address mapped to "huawei.com.cn" first. If receiving no response, the DNS client sends a query message containing "huawei" to the DNS server to search for the mapped IP address.

**Precautions**

The switch 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.

If **vpn-instance** *vpn-instance-name* is specified, the specified domain name suffix can be used to search for the IP address corresponding to a domain name only when users access the domain name from the specified VPN instance.

## Example

# Configure a domain name suffix as com.cn.

```
<HUAWEI> system-view
[HUAWEI] dns domain com.cn
```

# 6.5.7 dns resolve

## Function

The **dns resolve** command enables dynamic domain name resolution.

The **undo dns resolve** command disables dynamic domain name resolution.

By default, dynamic domain name resolution is disabled.

## Format

**dns resolve**

**undo dns resolve**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

To obtain IP addresses mapping domain names using the DNS server, run the **dns resolve** command to enable dynamic domain name resolution on the device.

## Example

# Enable dynamic domain name resolution.

```
<HUAWEI> system-view
[HUAWEI] dns resolve
```

# 6.5.8 dns server

## Function

The **dns server** command configures the IP address of a DNS server.

The **undo dns server** command deletes the IP address of a DNS server.

By default, no IP addresses of DNS servers are configured.

## Format

**dns server** *ip-address* [ **vpn-instance** *vpn-instance-name* ]

**undo dns server** *ip-address* [ **vpn-instance** *vpn-instance-name* ]

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *ip-address* | Specifies the IP address of a DNS server. | 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 name. |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

During dynamic domain name resolution, the DNS client can send a query packet to the DNS server, requesting for the IP address of the specified domain name. The DNS client sends a domain name resolution request to the DNS servers according to the order in which they were configured. If the domain name resolution request on the first DNS server times out, the device sends the request to the second DNS server.

If **vpn-instance** *vpn-instance-name* is specified, the system sends domain name resolution requests only to the DNS server bound to the specified VPN instance.

**Precautions**

A maximum of six DNS server IP (IPv4 and IPv6) addresses can be configured on the switch.

## Example

# Configure two DNS servers with the IP addresses 172.16.1.1 and 10.10.10.10.

```
<HUAWEI> system-view
[HUAWEI] dns server 172.16.1.1
[HUAWEI] dns server 10.10.10.10
```

# 6.5.9 dns server source-ip

## Function

The **dns server source-ip** command configures the source IP address for the DNS client to communicate with a server.

The **undo dns server source-ip** command deletes the source IP address for the DNS client to communicate with a server.

By default, no source IP address is configured for the DNS client to communicate with a server.

## Format

**dns server source-ip** *ip-address* [ **vpn-instance** *vpn-instance-name* ]

**undo dns server source-ip** [ **vpn-instance** *vpn-instance-name* ]

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *ip-address* | Specifies the source IP address for the DNS client to communicate with a server. | 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 name. |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

When the DNS client communicates with a server, the administrator can specify a source IP address for the client 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 client.

If **vpn-instance** *vpn-instance-name* is specified, the specified source IP address is used only when the device communicates with the DNS server bound to the specified VPN instance.

## Example

# Specify the source IP address 172.16.1.1 for the DNS client to communicate with a server.

```
<HUAWEI> system-view
[HUAWEI] dns server source-ip 172.16.1.1
```

# 6.5.10 ip host

## Function

The **ip host** command configures a static DNS entry.

The **undo ip host** command deletes a static DNS entry.

By default, no static DNS entry is configured.

## Format

**ip host** *host-name ip-address* [ **vpn-instance** *vpn-instance-name* ]

**undo ip host** *host-name* [ *ip-address* [ **vpn-instance** *vpn-instance-name* ] ]

## 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 (_). |
| *ip-address* | Specifies the IP address mapping the host name. | 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 name. |

## 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 one host name is mapped to multiple IP addresses, only the latest configuration takes effect.

## Example

# Configure a static DNS entry.

```
<HUAWEI> system-view
[HUAWEI] ip host www.example.com 10.10.10.4
```

# 6.5.11 reset dns dynamic-host

## Function

The **reset dns dynamic-host** command clears dynamic DNS entries.

## Format

**reset dns dynamic-host** [ **vpn-instance** *vpn-instance-name* | **all** ]

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **vpn-instance** *vpn-instance-name* | Clears dynamic DNS entries of a specified VPN instance. | The value must be an existing VPN instance name. |
| **all** | Clears all dynamic DNS entries, including both public and private DNS entries.<br>**NOTE**<br>If neither **vpn-instance** *vpn-instance-name* nor **all** is specified, only public dynamic DNS entries are cleared. | - |

## Views

User view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

After confirming the action of deleting dynamic DNS entries, you can run the **reset dns dynamic-host** command to delete them.

**Precautions**

Dynamic DNS entries cannot be restored after being deleted. Confirm the action before you run the command.

## Example

# Delete all dynamic DNS entries.

```
<HUAWEI> reset dns dynamic-host all
```

# 6.6 mDNS Gateway Configuration Commands

## 6.6.1 Command Support

Only the following switch models support mDNS Gateway:

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S

## 6.6.2 display mdns gateway

### Function

The **display mdns gateway** command displays the mDNS gateway configuration.

### Format

**display mdns gateway**

### Parameters

None

### Views

All views

### Default Level

1: Monitoring level

### Usage Guidelines

After the mDNS gateway is configured, you can run the **display mdns gateway** command to view the mDNS gateway configuration.

### Example

# Display the mDNS gateway configuration.

```
<HUAWEI> display mdns gateway
mDNS Information:
------------------------------------------------------------------------------
 mDNS Gateway Status        : Enable
 mDNS Source IP             : -
------------------------------------------------------------------------------
 Gateway Probe Vlan   : vlan50  vlan101
------------------------------------------------------------------------------
```

**Table 6-34** Description of the display mdns gateway command output

| Item | Description |
| --- | --- |
| mDNS Gateway Status | mDNS gateway status:<br>• Enable<br>• Disable<br>To enable the mDNS gateway, run the **mdns gateway enable** command. |
| mDNS Source IP | Source IP address in outgoing mDNS request packets when the mDNS gateway is configured to periodically discover services.<br>To specify the source IP address in outgoing mDNS request packets when the mDNS gateway is configured to periodically discover services, run the **mdns source ip** command. |
| Gateway Probe Vlan | ID of the VLAN where the mDNS gateway is enabled to periodically discover services.<br>To specify the ID of the VLAN where the mDNS gateway is enabled to periodically discover services, run the **mdns probe interval** command. |

# 6.6.3 display mdns gateway statistics

## Function

The **display mdns gateway statistics** command displays statistics on the mDNS gateway.

## Format

**display mdns gateway statistics**

## Parameters

None

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

During routine maintenance and fault location, you can run the **display mdns gateway statistics** command to view statistics on mDNS packets received and sent by the mDNS gateway in a given period of time.

To query statistics again, run the **reset mdns gateway statistics** command to clear existing statistics.

**NOTICE**

Cleared statistics on the mDNS gateway cannot be restored. Exercise caution when you use the **reset mdns gateway statistics** command.

## Example

# Display statistics on the mDNS gateway.

```
<HUAWEI> display mdns gateway statistics
mDNS Gateway Statistics:
-----------------------------------
 Received        : 1120
  Query          : 411
  Response       : 707
  Discarded      : 29                Query TimeOut : 22                Bad source IP :
2
   Bad Pkt Length: 3
   Others         : 2
 Sent             : 681
  Query          : 678
  Response       : 3
```

**Table 6-35** Description of the **display mdns gateway statistics** command output

| Item | Description |
| --- | --- |
| Received | Number of mDNS packets received by the mDNS gateway. |
| Query | Number of mDNS query packets received by the mDNS gateway. |
| Response | Number of mDNS response packets received by the mDNS gateway. |
| Discarded | Number of mDNS packets discarded by the mDNS gateway.<br>**NOTE**<br>This field is displayed only when the value is not 0. |
| Query TimeOut | Number of packets that are discarded after being accumulated in a queue for more than 5 seconds. |

| Item | Description |
| --- | --- |
| Bad source IP | Number of unicast packets that are sent by untrusted mDNS relay agents and discarded by the mDNS gateway.<br>**NOTE**<br>This field is displayed only when the value of the **Discarded** field is not 0. |
| Bad Pkt Length | Number of mDNS packets discarded because the packet length exceeds the upper limit.<br>**NOTE**<br>This field is displayed only when the value of the **Discarded** field is not 0. |
| Others | Number of mDNS packets discarded because of other reasons.<br>**NOTE**<br>This field is displayed only when the value of the **Discarded** field is not 0. |
| Sent | Number of mDNS packets sent by the mDNS gateway. |
| Query | Number of mDNS query packets sent by the mDNS gateway. |
| Response | Number of mDNS response packets sent by the mDNS gateway. |

# 6.6.4 display mdns group

## Function

The **display mdns group** command displays mDNS group information.

## Format

**display mdns group** [ **name** *group-name* | **user-vlan** *vlan-id* ]

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **name** *group-name* | Displays mDNS group information with a specified name.<br>If the mDNS group with the specified name is not created on the device, no information is displayed. | The mDNS group name must have been created. |
| **user-vlan** *vlan-id* | Displays mDNS group information with a specified user VLAN.<br>If the specified user VLAN is not used any mDNS group, no information is displayed. | The user VLAN must have been created. |

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

The device functioning as the mDNS gateway maintains service information lists of all service provisioning devices on a network, and it can use mDNS groups to isolate service resources to provide refined service management. You can run this command to check mDNS group information including the VLANs of the users and service provisioning devices added to the mDNS group.

If **name** *group-name* or **user-vlan** *vlan-id* is not specified in the command, the information about all mDNS groups is displayed.

## Example

# Display the information about all mDNS groups.

```
<HUAWEI> display mdns group
mDNS Group Information:
------------------------------------------------------------------------------
 Group Name   : group1
 User Vlan    : 10
 Service Vlan :  20  30

 Group Name   : group2
 User Vlan    : 20  30
 Service Vlan :  20  40
------------------------------------------------------------------------------
Total: 2
```

**Table 6-36** Description of the **display mdns group** command output

| Item | Description |
| --- | --- |
| Group Name | Name of an mDNS group.<br>To configure the mDNS group name, run the **mdns group** command. |
| User Vlan | VLAN that users in an mDNS group belong to.<br>To configure the VLAN that users in an mDNS group belong to, run the **user-vlan** command. |
| Service Vlan | VLAN that service provisioning devices in an mDNS group belong to.<br>To configure the VLAN that service provisioning devices in an mDNS group belong to, run the **service-vlan** command. |
| Total | Number of mDNS groups that have been configured on the device. |

## 6.6.5 display mdns service

### Function

The **display mdns service** command displays service information recorded on the mDNS gateway.

### Format

**display mdns service** { **all** [ **verbose** ] | **name** *name* | **vlan** *vlan-id* }

### Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **all** | Displays all service information recorded on the mDNS gateway. | - |
| **name** *name* | Displays information about a specified service name recorded on the mDNS gateway. | The service name must have been created. |

| Parameter | Description | Value |
| --- | --- | --- |
| **vlan** *vlan-id* | Displays service information provided by a specified service VLAN, which is recorded on the mDNS gateway.<br>The VLAN ID indicates the VLAN that the service provisioning device belongs to. | The service VLAN must have been created. |
| **verbose** | Displays detailed service information recorded on the mDNS gateway. If this parameter is not specified, the summary of service information recorded on the mDNS gateway is displayed. | - |

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

The device functioning as the mDNS gateway maintains service information lists of all service provisioning devices on a network. You can run this command to check service information recorded on the device.

NOTE

When a service name begins with a space or contains a question mark (?), the **name** parameter cannot be specified in this command.

## Example

# Display the summary of all services recorded on the mDNS gateway.

```
<HUAWEI> display mdns service all
MDNS Service Info:

Service name : Officejet Pro 8100 [C12FFA] (7)._printer._tcp.local
  SRV Info:
     Domain Name : HPC12FFA-156.local
     Port        : 515
     Vlan Id     : 200
  A Info:
     Domain Name : HPC12FFA-156.local
     IP Address  : 10.1.1.254
```

```
    Vlan Id     : 200
  TXT Info:
    Vlan Id     : 200
    Data Length : 297
Total service: 1
```

# Display the details of all services recorded on the mDNS gateway.

```
<HUAWEI> display mdns service all verbose
MDNS Service Info:

Service name : Officejet Pro 8100 [C12FFA] (7)._printer._tcp.local
  SRV Info:
    Domain Name : HPC12FFA-156.local
    Port        : 515
    Vlan Id     : 10
    Cache Flush : 1
    Class       : 1
    TTL         : 120
    Aging Time  : 95
    Data Length : 264
    Priority    : 0
    Weight      : 0
  A Info:
    Domain Name : HPC12FFA-156.local
    IP Address  : 10.1.1.254
    Vlan Id     : 10
    Cache Flush : 1
    Class       : 1
    TTL         : 120
    Aging Time  : 115
  TXT Info:
    Vlan Id     : 10
    Data Length : 297
    Cache Flush : 1
    Class       : 1
    TTL         : 4500
    Aging Time  : 3400
    Text        : ***
Total service: 1
```

**Table 6-37** Description of the **display mdns service** command output

| Item | Description |
| --- | --- |
| MDNS Service Info | Service information recorded on the mDNS gateway. |
| Service name | Service name recorded on the mDNS gateway. |
| SRV Info | SRV type information, indicating service record information. |
| Domain Name | Domain name corresponding to the service name. |
| Port | Number of the port that provides the service. |
| A Info | A type information, indicating host record information. |

| Item | Description |
| --- | --- |
| IP Address | IP address corresponding to the domain name. |
| TXT Info | TXT type information, indicating the description of service record information. |
| Data Length | TXT data length. |
| PTR Info | PTR type information, indicating that information is searched reversely; that is, the service provisioning device is searched based on the service type.<br>**NOTE**<br>This field is displayed only when the **display mdns service** command is run in the diagnostic view. |
| Total | Number of services recorded on the mDNS gateway.<br>● When you query all service information or service information provided by a specified service VLAN recorded on the mDNS gateway, this field displays the total number of service names.<br>● When you query service information about a specified service name recorded on the mDNS gateway, this field displays the sum of the SRV Info, TXT Info, and PTR Info field values. Type A information and type AAAA information are excluded because they are not service information. |
| Cache Flush | Cache information about services. The value can be 0 or 1.<br>● The value 1 indicates that the information is cached information.<br>● The value 0 indicates that the information is not cached information. |
| Class | Service type.<br>● 1: indicates the Internet type.<br>● 255: indicates any type. |
| TTL | TTL of the service. |

| Item | Description |
| --- | --- |
| Aging Time | Time elapsed after the mDNS gateway records the service information, in seconds. |
| Priority | Service priority. |
| Weight | Service weight. |
| Text | Service text. |
| Vlan Id | Service VLAN ID, indicating the VLAN that the service provisioning device belongs to. |

# 6.6.6 mdns gateway enable

## Function

The **mdns gateway enable** command enables the mDNS gateway.

The **undo mdns gateway enable** command disables the mDNS gateway.

By default, the mDNS gateway is disabled.

## Format

**mdns gateway enable**

**undo mdns gateway enable**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

### Usage Scenario

Bonjour technology proposed by Apple uses mDNS. The destination multicast address of 224.0.0.251 used by mDNS is only valid in a Layer 2 broadcast domain. That is, information can be forwarded in a VLAN only, but cannot be forwarded across VLANs or Layer 3 devices. Run the **mdns gateway enable** command on the

device to enable the mDNS gateway so that the device can discover services across VLANs or Layer 3. The mDNS gateway records all available service lists and responds to service requests from Bonjour-compliant terminals.

**Precautions**

The device cannot function as both mDNS relay and gateway. A protection failure will occur if the **mdns relay enable** and **mdns gateway enable** commands are both configured on the device.

## Example

# Enable the mDNS gateway.

```
<HUAWEI> system-view
[HUAWEI] mdns gateway enable
```

# 6.6.7 mdns group

## Function

The **mdns group** command creates an mDNS group and displays the mDNS group view.

The **undo mdns group** command deletes the created mDNS group.

By default, no mDNS group is created.

## Format

**mdns group** *group-name*

**undo mdns group** *group-name*

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *group-name* | Specifies the name of an mDNS group. | The value is a string of 1 to 31 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string. |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

By default, the mDNS gateway queries service information lists of all service provisioning devices when receiving an mDNS request packet from a user requesting for a service. The mDNS gateway then replies to the user with a message containing the service provisioning devices that can provide the service. All the service provisioning devices mapping the service are visible to the user; therefore, service resources cannot be isolated. You can configure an mDNS group on the mDNS gateway to implement service resource isolation and refined service management. After receiving an mDNS request packet from a user requesting for a service, the mDNS gateway queries the mDNS group based on the user VLAN. If the user VLAN is added to a certain mDNS group, the gateway queries and replies with the requested service from the service list provided by the service VLAN mapping the mDNS group. If no mDNS group is specified for the user VLAN or no service VLAN is configured in the mDNS group, the gateway queries and replies with the requested service from the service lists provided by all service VLANs.

**Follow-up Procedure**

- Run the **user-vlan** command to configure the user VLAN for the mDNS group.
- Run the **service-vlan** command to configure the service VLAN to provide services for the users in the mDNS group.

**Precautions**

The device supports a maximum of 4096 mDNS groups.

## Example

# Create an mDNS group named **group1**.

```
<HUAWEI> system-view
[HUAWEI] mdns group group1
```

# 6.6.8 mdns probe interval

## Function

The **mdns probe interval** command enables the device to periodically discover services and sets the discovery interval.

The **undo mdns probe interval** command disables the device from periodically discovering services and deletes the discovery interval.

By default, the device is not enabled to periodically discover services and the discovery interval is not set.

## Format

**mdns probe interval** *interval*

**undo mdns probe interval**

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *interval* | Specifies the discovery interval. | The value is an integer that ranges from 60 to 38400, in seconds. |

## Views

VLAN view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

This command is used on an mDNS gateway or mDNS relay. The mDNS gateway maintains service information lists of all service provisioning devices on the network. A service information list records the service name, service type, TTL, host name, and IP address of each service. The TTL is provided by a service provisioning device to the mDNS gateway, and represents the aging time of a service. If the mDNS gateway receives mDNS response packets from a service provisioning device within the aging time, the mDNS gateway updates its service information. If the mDNS gateway does not receive mDNS response packets from a service provisioning device within the aging time, the mDNS gateway deletes its service information. If an mDNS gateway already exists on the network, a service provisioning device connected to the network advertises service information to the mDNS gateway through the mDNS relay. If a service provisioning device already exists before an mDNS gateway connects to the network, the service provisioning device does not advertise service information to the mDNS gateway.

If the device works as an mDNS gateway, you can run the **mdns probe interval** command to enable the periodical service discovery function and set the service discovery interval. The device then sends a service query message at the specified interval, and updates the service information list after receiving a response message from the service provisioning device.

If the device works as an mDNS relay and the **mdns probe interval** command is run, the device sends a service query message at the specified interval to request available service update in its VLAN, and forwards the response message from the service provisioning device to the mDNS gateway, ensuring that service information lists on the mDNS gateway are updated immediately.

**Precautions**

When the device as the mDNS gateway and service provisioning device are located on different network segments, the mDNS relay but not the mDNS gateway needs to be configured to periodically update service lists.

Only the following types of services can be discovered:

- _services._dns-sd._udp.local
- _raop._tcp.local
- _airplay._tcp.local
- _printer._tcp.local
- _device-info._tcp.local
- _rfb._tcp.local
- _sftp-ssh._tcp.local
- _ssh._tcp.local
- _smb._tcp.local
- _afpovertcp._tcp.local
- _universal._sub._ipp._tcp.local

## Example

# Enable the device to periodically discover services in VLAN 100 and set the discovery interval to 150s.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] mdns probe interval 150
```

# 6.6.9 mdns permit service-type

## Function

The **mdns permit service-type** command configures the service type that can be recorded by an mDNS gateway.

The **undo mdns permit id** command cancels the configured service type that can be recorded by an mDNS gateway.

By default, an mDNS gateway can record all service types.

## Format

**mdns permit service-type** *service-type* **id** *id*

**undo mdns permit id** *id*

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **service-type** *service-type* | Specifies a service type. | The value can be any service type that service provider devices can provide. The value is a string of characters, including digits, case-insensitive letters, and special characters visible on the keyboard, such as underscores (_), periods (.), and hyphens (-). |
| **id** *id* | Specifies a service type ID. | The value is an integer that ranges from 0 to 99. |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

By default, an mDNS gateway records all service types on the network and generates a service list. Because a service list size is limited, some uncommonly used services occupy the list space, which may cause entries unable to be generated for commonly used services such as airplay and printer. To reduce the number of service entries in the service list, run the **mdns permit service-type** command. This command allows service entries to be generated for only the specified service type, reduces the number of service entries in the service list.

**NOTE**

- An mDNS gateway can be configured to record airplay and printer services (a maximum of 64 airplay and printer devices are allowed), meeting the requirements in high-density WLANs and enterprise office WLANs as well as the requirements in manufacturing, finance, and government sectors.
- An mDNS gateway can be configured to record airplay and printer services (a maximum of 256 airplay and printer devices are allowed), meeting the requirements in scenarios where the number of VLANs to which concurrent users belong is less than 36.

## Example

# Configure the service type that can be recorded by the mDNS gateway.

```
<HUAWEI> system-view
[HUAWEI] mdns permit service-type _raop._tcp.local id 0
[HUAWEI] mdns permit service-type _airplay._tcp.local id 1
```

```
[HUAWEI] mdns permit service-type _printer._tcp.local id 2
[HUAWEI] mdns permit service-type _device-info._tcp.local id 3
[HUAWEI] mdns permit service-type _rfb._tcp.local id 4
[HUAWEI] mdns permit service-type _sftp-ssh._tcp.local id 5
[HUAWEI] mdns permit service-type _ssh._tcp.local id 6
[HUAWEI] mdns permit service-type _smb._tcp.local id 7
[HUAWEI] mdns permit service-type _afpovertcp._tcp.local id 8
[HUAWEI] mdns permit service-type _universal._sub._ipp._tcp.local id 9
```

# 6.6.10 mdns source ip

## Function

The **mdns source ip** command configures the source IP address in mDNS packets sent by the device that functions as an mDNS gateway or mDNS relay.

The **undo mdns source ip** command deletes the configuration of the source IP address in mDNS packets sent by the device.

By default, no source IP address is configured.

## Format

**mdns source ip** *ip-address*

**undo mdns source ip**

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *ip-address* | Specifies a source IP address. | The value is in dotted decimal notation. |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

### Usage Scenario

To ensure normal communication with user terminals and service provisioning devices, run this command to specify the source IP address in mDNS packets sent by the mDNS gateway or mDNS relay.

NOTE

When the device works as an mDNS relay, it is recommended that the IP address of the interface connecting the device to the mDNS gateway be used as the source IP address.

User terminals and service provisioning devices will ignore the source IP address of multicast mDNS packets received from the mDNS gateway or mDNS relay. As such, the source IP address configured by this command does not need to be on the same network segment as the user terminals or service provisioning devices.

When the device functions as an mDNS gateway, the configured source IP address in mDNS packets sent by the device applies to the following scenarios:

- When the mDNS gateway is enabled to periodically discover services, it encapsulates mDNS query packets with the source IP address configured by this command, so that it can receive response packets from service provisioning devices. If this command is not run to configure the source IP address, the mDNS gateway uses the IP address of the VLANIF interface corresponding to the VLAN where the periodic service discovery function is enabled as the source IP address of mDNS packets.
- If an mDNS relay is deployed, the mDNS gateway exchanges packets with the mDNS relay in unicast mode. When sending packets to the mDNS relay, the mDNS gateway uses the next-hop IP address of the outbound interface as the source IP address of the packets based on the routing table. If this command is configured, the device preferentially uses the configured IP address as the source IP address of packets.
- When receiving a request to discover services from a terminal, the mDNS gateway uses the IP address configured by this command as the source IP address of the response packet. If this command is not run to configure the source IP address, the mDNS gateway uses the IP address of the VLANIF interface corresponding to the VLAN to which the response packet belongs as the source IP address of the response packet.

When the device functions as an mDNS relay, the configured source IP address in mDNS packets sent by the device applies to the following scenarios:

- When the mDNS relay is enabled to periodically discover services, it encapsulates mDNS query packets with the source IP address configured by this command, so that it can receive response packets from service provisioning devices. If this command is not run to configure the source IP address, the mDNS relay uses the IP address of the VLANIF interface corresponding to the VLAN where the periodic service discovery function is enabled as the source IP address of mDNS packets.
- When the device acting as the mDNS relay forwards mDNS packets to an mDNS gateway, it uses the next-hop IP address of the outbound interface as the source IP address of packets based on the routing table. If this command is configured, the device preferentially uses the configured IP address as the source IP address of packets.

**Precautions**

When the device acting as an mDNS gateway is configured to periodically discover services, the device periodically sends mDNS query packets to all mDNS service provisioning devices in the VLAN, which are expected to return response packets. The destination IP address is the multicast address 224.0.0.251.

Before the mDNS service TTL expires, the mDNS gateway sends mDNS query packets to service provisioning devices that are expected to return response

packets. If an mDNS service is advertised through an mDNS relay, the destination IP address of the query packets is the IP address of the mDNS relay. If an mDNS service is not advertised through an mDNS relay, the destination IP address is the multicast address 224.0.0.251.

When the device acting as an mDNS gateway receives mDNS requests from terminals and the requested services are available, the device returns mDNS response packets. If the mDNS request packets are forwarded through an mDNS relay, the destination IP address of the response packets is the IP address of the mDNS relay. If mDNS request packets are not forwarded through an mDNS relay, the destination IP address is the multicast address 224.0.0.251.

## Example

# Specify the source IP address of 10.1.1.1 in mDNS packets to be sent to periodically discover services and to be forwarded to the mDNS gateway by the device functioning as the mDNS relay.

```
<HUAWEI> system-view
[HUAWEI] mdns source ip 10.1.1.1
```

# 6.6.11 mdns whitelist source-ip

## Function

The **mdns whitelist source-ip** command enables the trusted mDNS relay agent function and configures the IP address of the trusted mDNS relay agent.

The **undo mdns whitelist source-ip** command deletes the IP address of the trusted mDNS relay agent.

By default, the trusted mDNS relay agent function is disabled.

## Format

**mdns whitelist source-ip** *ip-address*

**undo mdns whitelist source-ip** { **all** | *ip-address* }

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *ip-address* | Specifies the IP address of the trusted mDNS relay agent. | The value is in dotted decimal notation. |
| **all** | Deletes IP addresses of all trusted mDNS relay agents. | - |

## Views

System view

### Default Level

2: Configuration level

### Usage Guidelines

Bogus mDNS relay agents may exist on the network and forge mDNS packets, threatening network security. To prevent this problem, run the **mdns whitelist source-ip** command on the device functioning as the mDNS gateway to enable the trusted mDNS relay agent function and configure the IP address of the trusted mDNS relay agent. The device then only processes unicast packets from the trusted mDNS relay agent, and discards unicast packets from untrusted mDNS relay agents. If the mDNS relay agent and mDNS gateway are on different network segments, you need to run the **mdns whitelist source-ip** *ip-address* command on the mDNS gateway to specify the IP address of the mDNS relay agent.

### Example

# Configure the IP address 192.168.1.1 for the trusted mDNS relay agent.

```
<HUAWEI> system-view
[HUAWEI] mdns whitelist source-ip 192.168.1.1
```

## 6.6.12 reset mdns gateway statistics

### Function

The **reset mdns gateway statistics** command clears statistics on the mDNS gateway.

### Format

**reset mdns gateway statistics**

### Parameters

None

### Views

User view

### Default Level

3: Management level

### Usage Guidelines

During routine maintenance and fault location, you can view statistics on mDNS packets received and sent by the mDNS gateway in a given period of time. Before viewing the statistics, run the **reset mdns gateway statistics** command to delete

existing statistics. Then the mDNS gateway recollects statistics on received and sent mDNS packets. You can run the **display mdns gateway statistics** command to view statistics on mDNS packets received and sent by the mDNS gateway.

**NOTICE**

Cleared statistics on the mDNS gateway cannot be restored. Exercise caution when you use the **reset mdns gateway statistics** command.

### Example

# Clear statistics on the mDNS gateway.

```
<HUAWEI> reset mdns gateway statistics
```

## 6.6.13 service-vlan

### Function

The **service-vlan** command configures service VLANs (that the service provisioning devices belong to) to provide services for users in an mDNS group.

The **undo service-vlan** deletes the service VLANs that provide services for users in an mDNS group.

By default, no service VLAN is configured to provide services for users in an mDNS group.

### Format

**service-vlan** *vlan-id* &<1-32>

**undo service-vlan** { *vlan-id* &<1-32> | **all** }

### Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *vlan-id* | Specifies the ID of the VLAN that the service provisioning devices belong to. | The value is an integer in the range from 1 to 4094. |
| **all** | Specifies all service VLANs. | - |

### Views

mDNS group view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

The device functioning as an mDNS gateway maintains service information lists of all service provisioning devices on a network, and it can use mDNS groups to isolate service resources to provide refined service management. You can run the **service-vlan** command to configure service VLANs to provide services for users in the mDNS group. The users (specified using the **user-vlan** command in the mDNS group view) in the mDNS group can only obtain services from the service list provided by the service VLAN mapping the mDNS group.

**Prerequisites**

An mDNS group has been created using the **mdns group** command.

**Precautions**

- You can add at most 32 service VLANs to an mDNS group.
- You can add a service VLAN to multiple mDNS groups to provide services for the users in these groups.
- The service VLAN cannot be configured as a reserved VLAN for a stack.

## Example

# Configure the service provisioning devices in VLAN 10 to provide services for the mDNS group **group1**.

```
<HUAWEI> system-view
[HUAWEI] mdns group group1
[HUAWEI-mdns-group-group1] service-vlan 10
```

# 6.6.14 user-vlan (mDNS group view)

## Function

The **user-vlan** command configures user VLANs for an mDNS group.

The **undo user-vlan** command deletes user VLANs for the mDNS group.

By default, no user VLAN is configured for an mDNS group.

## Format

**user-vlan** *vlan-id* &<1-32>

**undo user-vlan** { *vlan-id* &<1-32> | **all** }

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *vlan-id* | Specifies the ID of the VLAN that users belong to. | The value is an integer that ranges from 1 to 4094. |
| **all** | Specifies all user VLANs. | - |

## Views

mDNS group view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

The device functioning as the mDNS gateway maintains service information lists of all service provisioning devices on a network, and it can use mDNS groups to isolate service resources to provide refined service management. You can run the **user-vlan** command to configure user VLANs for an mDNS group. The intra-VLAN users who join the mDNS group can only obtain services from the service list provided by the service VLAN (specified using the **service-vlan** command) mapping the mDNS group.

**Prerequisites**

An mDNS group has been created using the **mdns group** command.

**Precautions**

- You can add at most 32 user VLANs to an mDNS group.
- A user VLAN can belong to only one mDNS group.
- If no mDNS group is specified for the user VLAN or no service VLAN is configured in the mDNS group, the gateway queries and replies with the requested service from the service lists provided by all service VLANs.

## Example

# Add the users in VLAN 10 to the mDNS group **group1**.

```
<HUAWEI> system-view
[HUAWEI] mdns group group1
[HUAWEI-mdns-group-group1] user-vlan 10
```

# 6.7 mDNS Relay Configuration Commands

# 6.7.1 Command Support

Only the following switch models support mDNS Relay:

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S

# 6.7.2 display mdns relay

## Function

The **display mdns relay** command displays the mDNS relay configuration.

## Format

**display mdns relay**

## Parameters

None

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

After the mDNS relay is configured, you can run the **display mdns relay** command to view the mDNS relay configuration.

## Example

# Display the mDNS relay configuration.

```
<HUAWEI> display mdns relay
MDNS Relay Information:
-------------------------------------------------------------------------------
 MDNS Gateway IP   :  10.1.1.2
 MDNS Source IP    :  192.168.1.1
-------------------------------------------------------------------------------
 Relay Enable Vlan :  vlan100
-------------------------------------------------------------------------------
 Relay Probe Vlan  :  vlan100
-------------------------------------------------------------------------------
```

**Table 6-38** Description of the display mdns relay command output

| Item | Description |
| --- | --- |
| MDNS Gateway IP | IP address of the mDNS gateway specified on the device as the mDNS relay.<br>To specify the IP address of the mDNS gateway on the device as the mDNS relay, run the **mdns gateway ip** command. |
| MDNS Source IP | Source IP address in mDNS packets to be sent to periodically discover services and to be forwarded to the mDNS gateway by the device as the mDNS relay.<br>To specify the source IP address in mDNS packets to be sent to periodically discover services and to be forwarded to the mDNS gateway by the device as the mDNS relay, run the **mdns source ip** command. |
| Relay Enable Vlan | ID of the VLAN where the mDNS relay is enabled.<br>To enable the mDNS relay, run the **mdns relay enable** command. |
| Relay Probe Vlan | ID of the VLAN where the mDNS relay is enabled to periodically discover services.<br>To specify the ID of the VLAN where the mDNS relay is enabled to periodically discover services, run the **mdns probe interval** command. |

# 6.7.3 display mdns relay statistics

## Function

The **display mdns relay statistics** command displays statistics on the mDNS relay.

## Format

**display mdns relay statistics**

## Parameters

None

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

During routine maintenance and fault location, you can run the **display mdns relay statistics** command to view statistics on mDNS packets received, sent and dropped by the mDNS relay in a given period of time.

To query statistics again, run the **reset mdns relay statistics** command to clear existing statistics.

**NOTICE**

Cleared statistics on the mDNS relay cannot be restored. Exercise caution when you use the **reset mdns relay statistics** command.

## Example

# Display statistics on the mDNS relay.

```
<HUAWEI> display mdns relay statistics
MDNS relay statistics:
-------------------------------------
 Received  : 100
 Sent      : 100
 Dropped   : 0
  Bad Pkt Length : 0
  Other          : 0
-------------------------------------
```

**Table 6-39** Description of the display mdns relay statistics command output

| Item | Description |
| --- | --- |
| Received | Number of mDNS packets received by the mDNS relay. |
| Sent | Number of mDNS packets sent by the mDNS relay. |
| Dropped | Number of mDNS packets dropped by the mDNS relay. |
| Bad Pkt Length | Number of mDNS packets discarded because the packet length exceeds the upper limit. |
| Other | Number of mDNS packets discarded because of other reasons. |

# 6.7.4 mdns gateway ip

## Function

The **mdns gateway ip** command specifies the IP address of the mDNS gateway on the device as the mDNS relay.

The **undo mdns gateway ip** command deletes the configured IP address of the mDNS gateway on the device as the mDNS relay.

By default, the IP address of the mDNS gateway is not specified on the device as the mDNS relay.

## Format

**mdns gateway ip** *ip-address*

**undo mdns gateway ip**

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *ip-address* | Specifies the IP address of the mDNS gateway. | The value is in dotted decimal notation. |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

The device as the mDNS relay needs to forward mDNS packets from Bonjour-compliant terminals or service provisioning devices to the mDNS gateway. After the **mdns gateway ip** command is used to specify the IP address of the mDNS gateway on the mDNS relay, the mDNS relay converts mDNS packets from Bonjour-compliant terminals or service provisioning devices into unicast packets and sends them to the mDNS gateway.

## Example

# Specify the IP address of the mDNS gateway as 10.1.1.1 on the device as the mDNS relay.

```
<HUAWEI> system-view
[HUAWEI] mdns gateway ip 10.1.1.1
```

# 6.7.5 mdns probe interval

## Function

The **mdns probe interval** command enables the device to periodically discover services and sets the discovery interval.

The **undo mdns probe interval** command disables the device from periodically discovering services and deletes the discovery interval.

By default, the device is not enabled to periodically discover services and the discovery interval is not set.

## Format

**mdns probe interval** *interval*

**undo mdns probe interval**

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *interval* | Specifies the discovery interval. | The value is an integer that ranges from 60 to 38400, in seconds. |

## Views

VLAN view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

This command is used on an mDNS gateway or mDNS relay. The mDNS gateway maintains service information lists of all service provisioning devices on the network. A service information list records the service name, service type, TTL, host name, and IP address of each service. The TTL is provided by a service provisioning device to the mDNS gateway, and represents the aging time of a service. If the mDNS gateway receives mDNS response packets from a service provisioning device within the aging time, the mDNS gateway updates its service information. If the mDNS gateway does not receive mDNS response packets from a service provisioning device within the aging time, the mDNS gateway deletes its service information. If an mDNS gateway already exists on the network, a service provisioning device connected to the network advertises service information to the mDNS gateway through the mDNS relay. If a service provisioning device already

exists before an mDNS gateway connects to the network, the service provisioning device does not advertise service information to the mDNS gateway.

If the device works as an mDNS gateway, you can run the **mdns probe interval** command to enable the periodical service discovery function and set the service discovery interval. The device then sends a service query message at the specified interval, and updates the service information list after receiving a response message from the service provisioning device.

If the device works as an mDNS relay and the **mdns probe interval** command is run, the device sends a service query message at the specified interval to request available service update in its VLAN, and forwards the response message from the service provisioning device to the mDNS gateway, ensuring that service information lists on the mDNS gateway are updated immediately.

**Precautions**

When the device as the mDNS gateway and service provisioning device are located on different network segments, the mDNS relay but not the mDNS gateway needs to be configured to periodically update service lists.

Only the following types of services can be discovered:

- _services._dns-sd._udp.local
- _raop._tcp.local
- _airplay._tcp.local
- _printer._tcp.local
- _device-info._tcp.local
- _rfb._tcp.local
- _sftp-ssh._tcp.local
- _ssh._tcp.local
- _smb._tcp.local
- _afpovertcp._tcp.local
- _universal._sub._ipp._tcp.local

## Example

# Enable the device to periodically discover services in VLAN 100 and set the discovery interval to 150s.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] mdns probe interval 150
```

# 6.7.6 mdns relay enable

## Function

The **mdns relay enable** command enables the mDNS relay.

The **undo mdns relay enable** command disables the mDNS relay.

By default, the mDNS relay is disabled.

## Format

**mdns relay enable**

**undo mdns relay enable**

## Parameters

None

## Views

VLAN view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

Bonjour technology proposed by Apple uses mDNS. The destination multicast address of 224.0.0.251 used by mDNS is only valid in a Layer 2 broadcast domain. That is, information can be forwarded in a VLAN only, but cannot be forwarded across VLANs or Layer 3 devices. The mDNS relay and mDNS gateway solution implements service discovery across Layer 3. The device can function as the mDNS relay to forward mDNS packets exchanged between Bonjour-compliant terminals or service provisioning devices and mDNS gateway, implementing service discovery across Layer 3. The **mdns relay enable** command enables the mDNS relay.

**Precautions**

The device cannot function as both mDNS relay and gateway. A protection failure will occur if the **mdns relay enable** and **mdns gateway enable** commands are both configured on the device.

## Example

# Enable the mDNS relay.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] mdns relay enable
```

# 6.7.7 mdns source ip

## Function

The **mdns source ip** command configures the source IP address in mDNS packets sent by the device that functions as an mDNS gateway or mDNS relay.

The **undo mdns source ip** command deletes the configuration of the source IP address in mDNS packets sent by the device.

By default, no source IP address is configured.

## Format

**mdns source ip** *ip-address*

**undo mdns source ip**

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *ip-address* | Specifies a source IP address. | The value is in dotted decimal notation. |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

### Usage Scenario

To ensure normal communication with user terminals and service provisioning devices, run this command to specify the source IP address in mDNS packets sent by the mDNS gateway or mDNS relay.

**NOTE**

When the device works as an mDNS relay, it is recommended that the IP address of the interface connecting the device to the mDNS gateway be used as the source IP address.

User terminals and service provisioning devices will ignore the source IP address of multicast mDNS packets received from the mDNS gateway or mDNS relay. As such, the source IP address configured by this command does not need to be on the same network segment as the user terminals or service provisioning devices.

When the device functions as an mDNS gateway, the configured source IP address in mDNS packets sent by the device applies to the following scenarios:

- When the mDNS gateway is enabled to periodically discover services, it encapsulates mDNS query packets with the source IP address configured by this command, so that it can receive response packets from service provisioning devices. If this command is not run to configure the source IP address, the mDNS gateway uses the IP address of the VLANIF interface corresponding to the VLAN where the periodic service discovery function is enabled as the source IP address of mDNS packets.
- If an mDNS relay is deployed, the mDNS gateway exchanges packets with the mDNS relay in unicast mode. When sending packets to the mDNS relay, the mDNS gateway uses the next-hop IP address of the outbound interface as the source IP address of the packets based on the routing table. If this command

is configured, the device preferentially uses the configured IP address as the source IP address of packets.

- When receiving a request to discover services from a terminal, the mDNS gateway uses the IP address configured by this command as the source IP address of the response packet. If this command is not run to configure the source IP address, the mDNS gateway uses the IP address of the VLANIF interface corresponding to the VLAN to which the response packet belongs as the source IP address of the response packet.

When the device functions as an mDNS relay, the configured source IP address in mDNS packets sent by the device applies to the following scenarios:

- When the mDNS relay is enabled to periodically discover services, it encapsulates mDNS query packets with the source IP address configured by this command, so that it can receive response packets from service provisioning devices. If this command is not run to configure the source IP address, the mDNS relay uses the IP address of the VLANIF interface corresponding to the VLAN where the periodic service discovery function is enabled as the source IP address of mDNS packets.
- When the device acting as the mDNS relay forwards mDNS packets to an mDNS gateway, it uses the next-hop IP address of the outbound interface as the source IP address of packets based on the routing table. If this command is configured, the device preferentially uses the configured IP address as the source IP address of packets.

**Precautions**

When the device acting as an mDNS gateway is configured to periodically discover services, the device periodically sends mDNS query packets to all mDNS service provisioning devices in the VLAN, which are expected to return response packets. The destination IP address is the multicast address 224.0.0.251.

Before the mDNS service TTL expires, the mDNS gateway sends mDNS query packets to service provisioning devices that are expected to return response packets. If an mDNS service is advertised through an mDNS relay, the destination IP address of the query packets is the IP address of the mDNS relay. If an mDNS service is not advertised through an mDNS relay, the destination IP address is the multicast address 224.0.0.251.

When the device acting as an mDNS gateway receives mDNS requests from terminals and the requested services are available, the device returns mDNS response packets. If the mDNS request packets are forwarded through an mDNS relay, the destination IP address of the response packets is the IP address of the mDNS relay. If mDNS request packets are not forwarded through an mDNS relay, the destination IP address is the multicast address 224.0.0.251.

## Example

# Specify the source IP address of 10.1.1.1 in mDNS packets to be sent to periodically discover services and to be forwarded to the mDNS gateway by the device functioning as the mDNS relay.

```
<HUAWEI> system-view
[HUAWEI] mdns source ip 10.1.1.1
```

## 6.7.8 reset mdns relay statistics

### Function

The **reset mdns relay statistics** command clears statistics on the mDNS relay.

### Format

**reset mdns relay statistics**

### Parameters

None

### Views

User view

### Default Level

3: Management level

### Usage Guidelines

During routine maintenance and fault location, you can view statistics on mDNS packets received and sent by the mDNS relay in a given period of time. Before viewing the statistics, run the **reset mdns relay statistics** command to delete existing statistics. Then the mDNS relay recollects statistics on received and sent mDNS packets. You can run the **display mdns relay statistics** command to view statistics on mDNS packets received and sent by the mDNS relay.

**NOTICE**

Cleared statistics on the mDNS relay cannot be restored. Exercise caution when you use the **reset mdns relay statistics** command.

### Example

# Clear statistics on the mDNS relay.

```
<HUAWEI> reset mdns relay statistics
```

# 6.8 UDP Helper Configuration Commands

## 6.8.1 Command Support

Only the following switch models support UDP helper:

S5720I-SI, S5735-S, S5735-L, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S

# 6.8.2 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, the system displays the following information:

```
Info: Udp-helper has not been enabled, please enable udp-helper first.
```

## 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              Login Host Protocol
     53              Domain Name Server
     69              Trivial File Transfer
    137              NETBIOS Name Service
    138              NETBIOS Datagram Service
```

**Table 6-40** Description of the **display udp-helper port** command output

| Item | Description |
| --- | --- |
| Udp-Port-Number | UDP ports to which packets need to be relayed.<br>UDP ports are classified into the following types:<br>• Well-known port: The well-known port numbers range from 0 to 1023. These ports are used by standard TCP/UDP protocols.<br>• Registered port: The registered port numbers range from 1024 to 49151. They are vendor-specific ports.<br>• 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.<br>To configure the UDP ports, run the **udp-helper port** command. |
| Description | UDP port description. |

## 6.8.3 display udp-helper server

### Function

The **display udp-helper server** command displays the VLANIF interface, destination server address, and number of relayed UDP packets.

### 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.<br>• *interface-type* specifies the interface type.<br>• *interface-number* specifies the interface number. | The interface type must be VLANIF. |

## 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.

If no parameter is specified, statistics about relayed packets on all VLANIF interfaces are displayed.

NOTE

This command collects statistics on only the packets forwarded by the UDP helper server. Successful packet forwarding depends on the reachable route.

## Example

# Display statistics about relayed packets on VLANIF 100.

```
<HUAWEI> display udp-helper server interface vlanif 100
vlan-interface        Server-Ip          packet-num
Vlanif100          10.10.10.10                0
```

**Table 6-41** Description of the **display udp-helper server** command output

| Item | Description |
| --- | --- |
| vlan-interface | VLANIF interface on which UDP packets are relayed. |

| Item | Description |
| --- | --- |
| Server-Ip | Destination server address.<br>You can run the **udp-helper server** command to set the destination server address. |
| packet-num | Number of packets sent to the destination server. |

## 6.8.4 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

2: Configuration 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.

### 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
```

# 6.8.5 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 switch 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.

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 Time-to-Live (TTL) is larger than 1.
- The protocol type is UDP.
- The destination port is a specified UDP port.

**Precautions**

UDP helper enables a device to relay DHCP packets destined for UDP port 67 (that is, DHCP packets sent to the DHCP server).

However, a UDP helper-enabled device cannot relay DHCP packets destined for UDP port 68 (that is, DHCP packets sent to the DHCP client). To relay this type of DHCP packets, you must enable the DHCP relay function.

After the UDP Helper function is enabled, the switch relays broadcast packets destined for the following UDP ports by default.

| Protocol | UDP Port Number |
| --- | --- |
| Trivial File Transfer Protocol (TFTP) | 69 |
| Domain Name System (DNS) | 53 |
| Time Service | 37 |
| NetBIOS Name Service (NetBIOS-NS) | 137 |
| NetBIOS Datagram Service (NetBIOS-DS) | 138 |
| Terminal Access Controller Access Control System (TACACS) | 49 |

After UDP Helper is disabled, all specified UDP ports and default ports are canceled.

NOTE

After the UDP Helper function is enabled, the switch 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.

## Example

# Enable UDP Helper.

```
<HUAWEI> system-view
[HUAWEI] udp-helper enable
```

# 6.8.6 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 switch 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 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. | - |
| **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 switch relays the received UDP broadcast packets destined for the specified ports.

**Precautions**

The **udp-helper port** command takes effect globally. That is, if the switch is configured to relay packets destined for a UDP port, all the interfaces configured with the destination server address will relay such packets.

UDP helper enables a device to relay DHCP packets destined for UDP port 67 (that is, DHCP packets sent to the DHCP server).

However, a UDP helper-enabled device cannot relay DHCP packets destined for UDP port 68 (that is, DHCP packets sent to the DHCP client). To relay this type of DHCP packets, you must enable the DHCP relay function.

The switch supports a maximum of 16 UDP ports.

## Example

# Configure the switch to relay the broadcast packets destined for UDP port 100.

```
<HUAWEI> system-view
[HUAWEI] udp-helper enable
[HUAWEI] udp-helper port 100
```

# 6.8.7 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

VLANIF interface view

## Default Level

2: Configuration level

## 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.

**Precautions**

- A maximum of 20 destination servers can be configured on an interface. If multiple destination servers are configured on an interface, the switch 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 switch 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 VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] udp-helper server 10.1.1.2
```

# 6.9 IP Performance Optimization Configuration Commands

## 6.9.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

## 6.9.2 clear ip df

### Function

The **clear ip df** command enables fragmentation for outgoing control-plain IP packets on an interface.

The **undo clear ip df** command disables fragmentation for outgoing control-plain IP packets on an interface.

By default, fragmentation for outgoing control-plain IP packets on an interface is disabled.

### Format

**clear ip df**

**undo clear ip df**

### Parameters

None

### Views

Interface view

### Default Level

2: Configuration level

### Usage Guidelines

**Usage Scenario**

An IP header contains a Don't Fragment (DF) bit to identify whether packet fragmentation is allowed. Commonly, if the DF bit of a packet is set to 1, the packet cannot be fragmented. When the remote device or intermediate forwarding device receives IP packets, if it checks the packet length and discards packets whose length is longer than the Maximum Transmission Unit (MTU) on the interface, network communication is interrupted. You can run the **clear ip df**

command to enable fragmentation for outgoing control-plane IP packets so that packets with the DF bit set to 1 are fragmented based on the MTU value on the interface.

After fragmentation for outgoing control-plain IP packets is enabled on an interface, 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.

**Precautions**

This command takes effect only for the control-plain packets but not for the forwarding-plain packets.

## Example

# Enable fragmentation for outgoing IP packets on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] clear ip df
```

# Enable fragmentation for outgoing IP packets on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] clear ip df
```

# 6.9.3 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.

By default, the device processes packets sent to the CPU based on route options contained in these packets.

## Format

**discard { ra | rr | srr | ts }**

**undo discard { ra | rr | srr | ts }**

## Parameters

None

## Views

Interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

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.

**Precautions**

The **discard { ra | rr | srr | ts }** command only takes effect for the packets on inbound interfaces.

The **discard { ra | rr | srr | ts }** command only takes effect for packets sent to the CPU. For packets that are not sent to the CPU, the device processes and forwards them using the same method of processing packets without route options regardless of whether the **discard { ra | rr | srr | ts }** command is configured or not.

## Example

# Configure the device to discard the packets that contain the route alert option on the interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] discard ra
```

# Configure the device to discard the packets that contain the route alert option on the interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] discard ra
```

# 6.9.4 display icmp statistics

## Function

The **display icmp statistics** command displays ICMP traffic statistics.

## Format

**display icmp statistics**

## Parameters

None

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

To view information about ICMP packet sending and receiving, run the **display icmp statistics** command.

## 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 6-42** 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. |

| 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 requests | Number of multicast ping request packets. |
| Mping reply | Number of multicast ping reply packets. |

## 6.9.5 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* ]

**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. | - |

| Parameter | Description | Value |
| --- | --- | --- |
| **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.<br>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.
- Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support sub-interfaces.

## Example

# Display IP information about VLANIF15.

```
<HUAWEI> display ip interface vlanif 15
Vlanif15 current state : UP
Line protocol current state : UP
The Maximum Transmit Unit : 1500 bytes
input packets : 766390, bytes : 41540847, multicasts : 681817
```

```
output packets : 242239, bytes : 14679482, multicasts : 172333
Directed-broadcast packets:
 received packets:            0, sent packets:           0
 forwarded packets:           0, dropped packets:        0
Internet Address is 10.1.1.119/24
Broadcast address : 10.1.1.255
TTL being 1 packet number:    164035
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 6-43** Description of the **display ip interface** command output

| Item | Description |
| --- | --- |
| Vlanif15 current state | Physical status of the interface:<br>• UP: indicates that the interface is physically Up.<br>• DOWN: indicates that the interface is physically Down.<br>• Administratively down: indicates that the administrator has run the **shutdown (interface view)** command on the interface. |
| Line protocol current state | Link layer protocol status of the interface:<br>• UP: The link layer protocol of the interface is running properly.<br>• DOWN: The link layer protocol of the interface is Down or no IP address is configured on the interface. |
| The Maximum Transmit Unit | MTU of the interface. The default MTU of an Ethernet interface or a serial 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 : 766390, bytes : 41540847, multicasts : 681817 | Total number of packets, bytes, and multicast packets received by the interface. |

| Item | Description |
| --- | --- |
| output packets : 242239, bytes : 14679482, multicasts : 172333 | 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. |
| Internet Address is | IP address assigned to the interface and mask length. |
| Broadcast address | Broadcast address of the 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. |
| 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 VLANIF15.

```
<HUAWEI> display ip interface brief vlanif 15
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
Interface                   IP Address/Mask      Physical   Protocol
Vlanif15                    10.1.1.119/24        up         up
```

**Table 6-44** 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 | ^down: indicates that the interface is a backup interface. |
| (l): loopback | The letter "l" refers to loopback. |
| (s): spoofing | The letter "s" refers to spoofing. |
| (E): E-Trunk down | Indicates that the Eth-Trunk is Down because of the protocol negotiation on the E-Trunk. |
| Interface | Interface type and number. |
| IP Address/Mask | IP address and mask of an interface. |
| Physical | Physical status of an interface:<br>• Up: indicates that the interface is physically Up. (l) indicates that the loopback function is configured on the interface.<br>• Down: indicates that the interface becomes faulty.<br>• *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.<br>• !down: indicates that the FIB module is suspended. In this case, the link protocol status of the interface is Down. |

| Item | Description |
| --- | --- |
| Protocol | Link protocol status of the interface:<br>• 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.<br>• Down: indicates that the link protocol of the interface fails or no IP address is configured on the interface.<br>(l) indicates that the loopback function is configured on the interface. |

## 6.9.6 display ip forwarding status

### Function

The **display ip forwarding status** command displays whether IPv4 Layer 3 unicast forwarding is enabled on a switch.

### Format

**display ip forwarding status**

### Parameters

None

### Views

All views

### Default Level

1: Monitoring level

### Usage Guidelines

You can run this command to check whether IPv4 Layer 3 unicast forwarding is enabled on a switch.

### Example

# Display whether IPv4 Layer 3 unicast forwarding is enabled on the switch.

```
<HUAWEI> display ip forwarding status
Current IP forwarding status: Open
```

**Table 6-45** Description of the **display ip forwarding status** command output

| Item | Description |
| --- | --- |
| Current IP forwarding status | Whether IPv4 Layer 3 unicast forwarding is enabled:<br>• Open: The function is enabled.<br>• Closed: The function is disabled.<br>To configure IPv4 Layer 3 unicast forwarding, run the **ip forwarding disable** command. |

# 6.9.7 display ip socket

## Function

The **display ip socket** command displays information about the created IPv4 sockets.

## Format

**display ip socket** [ **monitor** ] [ **task-id** *task-id* **socket-id** *socket-id* | **socket-type** *socket-type* ]

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **monitor** | Displays information about the socket monitor. Information about the socket monitor is displayed together with information about the socket. | - |
| **task-id** *task-id* | Displays socket information of the task with a specified ID. | The value must be an existing task ID. |
| **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 6-46** shows the value range. |

**Table 6-46** 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 sockets.

```
<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,
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 = 0000-00-00 00:00:00+08:00, 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 = 0000-00-00 00:00:00+00:00, 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 = 0000-00-00 00:00:00+00:00, lost msg = 0, msg type = 0x00000000;
```

# Display the information about the IP socket with the task ID as 23 and socket ID as 1.

```
<HUAWEI> display ip socket monitor task-id 23 socket-id 1
Task = RSVP(23), socketid = 1, Proto = 46,
LA = 0.0.0.0, FA = 0.0.0.0,
sndbuf = 4194304, rcvbuf = 4194304, sb_cc = 0, rb_cc = 0,
socket option = 0,
socket state = SS_PRIV SS_NBIO SS_ASYNC
                    Socket Monitor:
Statistics:
 input packets = 0,recv packets = 0,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;
```

# Display information about the IP socket with the socket type as TCP.

```
<HUAWEI> display ip socket monitor socket-type 1
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_REUSEPORT SO_SENDVPNID(14849)
SO_SETKEEPALIVE,
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 = 0000-00-00 00:00:00+00:00, lost msg= 0, msg type=0x00000000;
Nothing else has been captured!
```

**Table 6-47** Description of the **display ip socket** command output

| Item | Description |
| --- | --- |
| SOCK_STREAM | Socket types. There are the following socket types:<br>• SOCK_STREAM<br>• SOCK_DGRAM<br>• SOCK_RAWLINK<br>• SOCK_RAWIP |
| Task | Type and ID of the task that invokes the socket. For example, Task = VTYD(30) indicates that the task named VTYD uses the socket, with the task ID being 30. |
| socketid | Socket ID. |

| Item | Description |
| --- | --- |
| Proto | Protocol number. |
| LA | Local address/port number. |
| FA | Remote address/port number. |
| 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. |

| Item | Description |
| --- | --- |
| socket option | Set socket options. There are the following socket options:<br>• SO_DEBUG: indicates that debugging is enabled.<br>• SO_ACCEPTCONN: indicates that the socket is the server and is responsible for monitoring.<br>• SO_REUSEADDR: indicates that addresses are overlapped. After the option is set, multiple identical addresses can be bound to an interface.<br>• SO_KEEPALIVE: indicates that the keepalive timer starts after a TCP connection is set up.<br>• SO_DONTROUTE: indicates that a socket must choose the direct route to the destination when setting up a connection.<br>• SO_BROADCAST: indicates that an interface can send broadcast packets.<br>• 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.<br>• SO_UDPCHECKSUM: indicates that the socket calculates the checksum of UDP packets.<br>• SO_SENDVPNID: indicates an exclusive option for VPNs.<br>• SO_SETKEEPALIVE: indicates that the keepalive timer starts after a TCP connection is set up.<br>• SO_SETACL: indicates that an ACL can be configured on the interface.<br>• SO_USELOOPBACK: indicates that a socket can use a loopback interface to receive or send data.<br>• 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. |

| Item | Description |
| --- | --- |
| | • SO_OOBINLINE: indicates out-band data. When receiving data, a socket processes the out-band data first.<br>• SO_SENDDATAIF: indicates that a socket uses the specified interface to receive or send data.<br>• SO_SENDDATAIF_DONTSETTTL: indicates that a socket uses the specified interface to receive or send data but does not set the TTL value.<br>• SO_SETSRCADDR: indicates that a socket sets the source address of outgoing packets.<br>• SO_SENDBY_IF_NEXTHOP: indicates that a socket sets the outbound interface and next hop address of outgoing packets. |

| Item | Description |
| --- | --- |
| socket state | Socket status. There are the following socket states:<br>• SS_NOFDREF: indicates that the socket ID is deleted.<br>• SS_ISCONNECTED: indicates that a TCP connection is set up.<br>• SS_ISCONNECTING: indicates that a TCP connection is being set up.<br>• SS_ISDISCONNECTING: indicates that a TCP connection is being closed.<br>• SS_CANTSENDMORE: indicates that a socket cannot send data.<br>• SS_CANTRCVMORE: indicates that a socket cannot receive data.<br>• SS_RCVMARK: indicates that a socket sets the receiving option in the received packet.<br>• SS_NBIO: indicates that the type of a socket is non-blocking.<br>• SS_ISCONFIRMING: indicates that the upper-layer application will complete processing a connection.<br>• SS_BLOCKING: indicates that congestion occurs during packet receiving and sending.<br>• SS_RECALL: indicates that the message notification method is set by an asynchronous socket.<br>• SS_PRIV: indicates the option transferred from the Unix. The option is invalid in the current socket.<br>• SS_ASYNC: indicates the status identifier of an asynchronous socket. |
| Asyn Que status | Current asynchronous queue status. |
| read | Number of messages read by the asynchronous queue. |
| write | Number of messages written by the asynchronous queue. |
| connect | Number of connection messages in the asynchronous queue. |
| close | Number of messages about closed connections in the asynchronous queue. |

| Item | Description |
| --- | --- |
| peer close | Number of messages about connections closed by the remote end in the asynchronous queue. |
| accept | Number of messages received by the asynchronous queue. |
| keep alive down | Number of keepalivedown messages in the asynchronous queue. |
| cram time | Time for the asynchronous queue to become full. |
| lost msg | Number of asynchronous messages discarded by the asynchronous queue. |
| msg type | Current asynchronous message type. |
| smb input | Number of times of notifying the application layer to read received packets on the backup board. |
| smb output | Number of times of notifying the application layer to read sent packets on the backup board. |
| smooth over | Number of times of notifying the application layer that the smoothing is over. |

# 6.9.8 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.

## Format

**display ip socket register-port**

## Parameters

None

## Views

All views

## Default Level

3: Management 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
5247      CWP_FWD     UDP4
31009     MPLSFW      UDP4
38514     INFO        UDP4
60000     EZOP        UDP4
65030     ipfpm       UDP4
65531     CWP_FWD     UDP4
65532     CWP_FWD     UDP4
65533     CWP_FWD     UDP4
65534     CWP_FWD     UDP4
3232      mdt         UDP6
3503      MPLSFW      UDP6
3784      BFD         UDP6
4784      BFD         UDP6
5246      CWP_FWD     UDP6
5247      CWP_FWD     UDP6
31009     MPLSFW      UDP6
38514     INFO        UDP6
60000     EZOP        UDP6
65531     CWP_FWD     UDP6
65532     CWP_FWD     UDP6
65533     CWP_FWD     UDP6
65534     CWP_FWD     UDP6
```

**Table 6-48** 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. |
| Type | Port type, including TCP and UDP. |

# 6.9.9 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              263482      local              263473
            bad protocol         0      bad format             1
            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              303399
            dropped          56479      no route             225
 Fragment:  input                0      output                 0
            dropped              0
            fragmented           0      couldn't fragment      0
 Reassembling:sum                0      timeouts               0
```

**Table 6-49** Description of the **display ip statistics** command output

| Item | Description |
| --- | --- |
| Input | Received packets. |
| sum | Total number of packets. |

| Item | Description |
| --- | --- |
| 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. |
| fragmented | Number of successfully fragmented packets. |
| couldn't fragment | Number of packets that cannot be fragmented. |

| Item | Description |
| --- | --- |
| Reassembling:sum | Number of successfully reassembled fragments. |
| timeouts | Number of expired fragments. |

# 6.9.10 display load-balance mode

## Function

The **display load-balance mode** command displays the load balancing mode on a switch.

## Format

**display load-balance mode** [ **packet** | **flow** | **slot** *slot-number* ]

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **packet** | Displays information about the switch adopting the per packet load balancing mode. | - |
| **flow** | Displays information about the switch adopting the per flow load balancing mode. | - |
| **slot** *slot-number* | Specifies the ID of a slot. After the slot ID is specified, the load balancing mode on a specified switch is displayed. | The value is an integer. It has a fixed value of 0 in a non-stack scenario, and depends on the device configuration in a stack scenario. |

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

Using the **display load-balance mode packet** or the **display load-balance mode flow** command displays information about the switch adopting the specified load balancing mode.

The **display load-balance mode slot** *slot-number* command displays the load balancing mode on a specified switch.

If neither the slot ID nor load balancing mode is specified in the **display load-balance mode** command, by default, load balancing mode on the switch is displayed.

## Example

# Display the load balancing modes on the switch.

```
<HUAWEI> display load-balance mode
load-balance flow slot 0
```

**Table 6-50** Description of the **display load-balance mode** command output

| Item | Description |
| --- | --- |
| load-balance | Load balancing mode:<br>• packet: per packet load balancing<br>• flow: per flow load balancing |
| slot | Slot ID. |

# 6.9.11 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. | - |

| Parameter | Description | Value |
| --- | --- | --- |
| **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

You can run the **display network status** command to check the network status, such as the running ports and services on the network. For example, when you find that a port is being used by an unknown module during a security scan, run the **display network status** command to check out the module.

## Example

# Display all information about the network 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
UDP   CMRE/1      0.0.0.0:65311            0.0.0.0:0
UDP6  AGT6/1      ::->161                  ::->0
UDP6  RDS /2      ::->1812                 ::->0
```

**Table 6-51** Description of the **display network status** command output

| Item | Description |
| --- | --- |
| Proto | Protocol |

| Item | Description |
| --- | --- |
| Task/SockId | Task and Socket ID<br>• VTYD: Process login requests of all users.<br>• HTTP: Transfer hypertext from WWW servers to local browsers<br>• AGNT: Implement the IPv4 SNMP protocol.<br>• SLAG: Implement E-Trunk.<br>• RDS: Implement the RADIUS protocol, manage the protocol state machine, and maintain protocol databases.<br>• CMRE: Register with the iMaster NCE-Campus for authentication and establishes NETCONF transmission channels.<br>• AGT6: Implement the IPv6 SNMP protocol. |
| Local Addr&Port | Local IP address and Port number |
| Foreign Addr&Port | Remote IP address and Port number |
| State | Connection status |

# 6.9.12 display priority

## Function

Using the **display priority** command, you can view the 802.1p priority and DSCP priority that are set in the system.

## Format

**display priority** { **8021p** | **dscp** }

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **8021p** | Displays the 802.1p priority. | - |
| **dscp** | Displays the DSCP priority. | - |

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

This command displays the 802.1p priority and DSCP priority that are set in the system.

The **display priority** command displays information only after the **set priority** command is executed to set the 802.1p priority or DSCP priority.

## Example

# Set the DSCP priority to 10, and display the DSCP priority set in the system.

```
<HUAWEI> system-view
[HUAWEI] set priority dscp 10
[HUAWEI] quit
<HUAWEI> display priority dscp
 The dscp priority is 10
```

# 6.9.13 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, RSVP, OSPF, 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 display application-specific RawIP packet statistics. The applications can be ICMP, RSVP, OSPF, and others.

**Precautions**

The number of packets received by a switch 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 6-52** Description of the **display rawip statistics** command output

| Item | Description |
| --- | --- |
| Received packets | Indicates the number of 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. |

# 6.9.14 display tcp statistics

## Function

The **display tcp statistics** command displays TCP traffic statistics.

## Format

**display tcp statistics**

## Parameters

None

## 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
```

**Table 6-53** 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. |

| Item | Description |
| --- | --- |
| 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. |
| Other information | Other information. |
| 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. |

# 6.9.15 display tcp status

## Function

The **display tcp status** command displays current TCP connection status.

## 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.
- 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
```

**Table 6-54** 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. |

| Field | Description |
| --- | --- |
| 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. |
| VPNID | ID of the VPN instance to which the TCP connection belongs.<br>● -1: indicates all VPNs.<br>● 0: indicates the public VPN.<br>● Other values: indicates the private VPN. The VPNID is defined by users. |
| State | TCP connection status:<br>● Closed: indicates that the TCP connection is closed.<br>● Listening: indicates that the TCP connection is being monitored.<br>● Syn_Rcvd: indicates that a packet with the SYN flag is received.<br>● Syn_Sent: indicates that a SYN packet is sent.<br>● Established: indicates that the TCP connection has been set up.<br>● 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.<br>● 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.<br>● Fin_Wait2: indicates that a user receives an ACK packet that responds to the sent packet with the FIN flag.<br>● 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.<br>● Closing: indicates that the user and server close the TCP connection simultaneously. |

# 6.9.16 display udp statistics

## Function

The **display udp statistics** command displays UDP traffic statistics.

## Format

**display udp statistics**

## 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 6-55** Description of the **display udp statistics** command output

| Item | Description |
| --- | --- |
| Received packet:<br>Total<br>Total (64bit high-capacity counter) | Total number of received UDP packets.<br>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. |

| Item | Description |
| --- | --- |
| 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. |
| 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:<br>Total<br>Total (64bit high-capacity counter) | Total number of sent UDP packets.<br>Total number of sent UDP packets (using the 64-bit counter). |

# 6.9.17 drop illegal-dst-ip enable

## Function

The **drop illegal-dst-ip enable** command enables the device to discard IP packets with invalid destination IP addresses and record logs.

The **undo drop illegal-dst-ip enable** command disables the device from discarding IP packets with invalid destination IP addresses and recording logs.

By default, a device is disabled from discarding IP packets with invalid destination IP addresses and recording logs.

## Format

**drop illegal-dst-ip enable**

**undo drop illegal-dst-ip enable**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

The following three types of IP addresses are invalid destination IP addresses and should not be used on the network:

- IP address with all 0s, that is, 0.0.0.0
- IP addresses with a network ID of 127, that is, 127.0.0.0 to 127.255.255.255
- Class E IP addresses except 255.255.255.255, that is, 240.0.0.0 to 255.255.255.254

After the **drop illegal-dst-ip enable** command is run on a device, the device discards the IP packets destined to invalid IP addresses and reports statistics about the discarded packets through logs. This reduces the device burden and prevents these packets from occupying network bandwidth.

NOTE

- Devices of the following models will discard IP packets destined to 0.0.0.0, 127.0.0.0 to 127.255.255.255, and 240.0.0.0 to 255.255.255.254 only after this function is configured:

  S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S
- Devices of other models discard the IP packet destined to an IP address that does not match any routing entry. Since there is no routing entry matching 0.0.0.0, 127.0.0.0 to 127.255.255.255, or 240.0.0.0 to 255.255.255.254, devices will discard IP packets destined to these IP addresses by default.

## Example

# Enable the device to discard IP packets with invalid destination IP addresses and record logs.

```
<HUAWEI> system-view
[HUAWEI] drop illegal-dst-ip enable
```

# 6.9.18 drop illegal-ip disable

## Function

The **drop illegal-ip disable** command disables a device from discarding IPv4 and IPv6 packets sourced from the all-zero address.

The **undo drop illegal-ip disable** command enables a device to discard IPv4 and IPv6 packets sourced from the all-zero address.

By default, the function of discarding IPv4 and IPv6 packets sourced from the all-zero address is enabled.

NOTE

The **drop illegal-ip disable** and **undo drop illegal-ip disable** commands are supported only by the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S. The other device models discard IPv4 and IPv6 packets sourced from the all-zero address by default, and this function cannot be disabled on those models.

## Format

**drop illegal-ip disable**

**undo drop illegal-ip disable**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

IPv4 and IPv6 packets sourced from the all-zero address are typical attack packets. You can run the **undo drop illegal-ip disable** command to enable a device to discard these packets.

## Example

# Enable a device to discard IPv4 and IPv6 packets sourced from the all-zero address.

```
<HUAWEI> system-view
[HUAWEI] undo drop illegal-ip disable
```

# 6.9.19 icmp blackhole unreachable send

## Function

The **icmp blackhole unreachable send** command enables the switch 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 switch from sending a Destination Unreachable ICMP packet to an initiator when a tracert packet matches an IPv4 blackhole route.

By default, the switch 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

## Usage Guidelines

If static IPv4 blackhole routes are configured on the switch configured with the user access and authentication function, when a user goes offline, only the IPv4 blackhole route corresponding to the user's address segment exists on the switch. When a tracert packet matches the IPv4 blackhole route, the switch 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 switch 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.

## Example

# Enable the switch 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
```

# 6.9.20 icmp host-unreachable send

## Function

The **icmp host-unreachable send** command enables the switch to send ICMP Host Unreachable packets.

The **undo icmp host-unreachable send** command disables the switch from sending ICMP Host Unreachable packets.

By default, the function of sending ICMP Host Unreachable packets is enabled.

## Format

**icmp host-unreachable send**

**undo icmp host-unreachable send**

## Parameters

None

## Views

System view, interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

ICMP error packets contain network information, such as network connectivity, host reachability, and route availability. ICMP error packets are ultimately returned to the sender because the sender is the logical receiver of the ICMP error packets. The sender learns about the error types from the ICMP error packets, and then determines how to retransmit the data.

The Destination Unreachable packets facilitate network control and management. However, the inherent defects of the ICMP protocol make the routing devices and hosts be prone to attacks. Therefore, sending the ICMP Destination Unreachable packets has the following defects:

- The ICMP packets increase traffic volume and burden the network devices.
- If a device receives a large number of malicious attack packets and needs to return ICMP error packets, the device is busy handling ICMP packets, and the device performance is degraded.
- The ICMP Destination Unreachable packets indicate that the destination is unreachable. If there are malicious attacks, user terminals cannot normally use the network.

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.

**Precautions**

The **icmp host-unreachable send** command can be run in the system view or interface view.

- After the function of sending ICMP Host Unreachable packets is disabled in the system view, all interfaces do not send ICMP Host Unreachable packets. Even if the function is enabled on an interface, the interface does not send ICMP Host Unreachable packets.
- After the function of sending ICMP Host Unreachable packets is enabled in the system view, all interfaces send ICMP Host Unreachable packets because the function is enabled on all interfaces by default. You can run the **undo icmp host-unreachable send** command in interface view to disable the function on a specified interface.

If the function of sending ICMP Host Unreachable packets is disabled, the switch does not send ICMP Host Unreachable packets in any situations.

This command needs to be configured on the inbound interface of ICMP packets in the interface view.

## Example

# Enable the switch to send ICMP Host Unreachable packets.

```
<HUAWEI> system-view
[HUAWEI] icmp host-unreachable send
```

# Enable VLANIF100 to send ICMP Host Unreachable packets.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] icmp host-unreachable send
```

# Enable GE0/0/1 to send ICMP Host Unreachable packets.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] icmp host-unreachable send
```

# 6.9.21 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 sends ICMP Port Unreachable packets.

## Format

**icmp port-unreachable send**

**undo icmp port-unreachable send**

## Parameters

None

## Views

System view, interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

ICMP error packets contain network information, such as network connectivity, host reachability, and route availability. ICMP error packets are ultimately returned to the sender because the sender is the logical receiver of the ICMP error packets. The sender learns about the error types from the ICMP error packets, and then determines how to retransmit the data.

The Destination Unreachable packets facilitate network control and management. However, the inherent defects of the ICMP protocol make the routing devices and

hosts be prone to attacks. Therefore, sending the ICMP Destination Unreachable packets has the following defects:

- The ICMP packets increase traffic volume and burden the network devices.
- If a device receives a large number of malicious attack packets and needs to return ICMP error packets, the device is busy handling ICMP packets, and the device performance is degraded.
- The ICMP Destination Unreachable packets indicate that the destination is unreachable. If there are malicious attacks, user terminals cannot normally use the network.

After you run the **undo icmp port-unreachable send** command, the device does not send ICMP Port Unreachable packets externally. This prevents the peer device from processing a large number of ICMP packets.

**Precautions**

The **icmp port-unreachable send** command can be run in the system view or interface view.

- After the function of sending ICMP Port Unreachable packets is disabled in the system view, all interfaces do not send ICMP Port Unreachable packets. Even if the function is enabled on an interface, the interface does not send ICMP Port Unreachable packets.
- After the function of sending ICMP Port Unreachable packets is enabled in the system view, all interfaces send ICMP Port Unreachable packets because the function is enabled on all interfaces by default. You can run the **undo icmp port-unreachable send** command in interface view to disable the function on a specified interface.

If the function of sending ICMP Port Unreachable packets is disabled, the switch does not send ICMP Port Unreachable packets in any situations.

## Example

# Enable the device to send ICMP Port Unreachable packets.

```
<HUAWEI> system-view
[HUAWEI] icmp port-unreachable send
```

# Enable the device to send ICMP Port Unreachable packets on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] icmp port-unreachable send
```

# Enable the device to send ICMP Port Unreachable packets on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] icmp port-unreachable send
```

# 6.9.22 icmp protocol-unreachable send

## Function

The **icmp protocol-unreachable send** command enables the function of sending ICMP Protocol Unreachable packets.

The **undo icmp protocol-unreachable send** command disables the function of sending ICMP Protocol Unreachable packets.

By default, the function of sending ICMP Protocol Unreachable packets is enabled.

## Format

**icmp protocol-unreachable send**

**undo icmp protocol-unreachable send**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

ICMP error packets contain network information, such as network connectivity, host reachability, and route availability. ICMP error packets are ultimately returned to the sender because the sender is the logical receiver of the ICMP error packets. The sender learns about the error types from the ICMP error packets, and then determines how to retransmit the data.

The Destination Unreachable packets facilitate network control and management. However, the inherent defects of the ICMP protocol make the routing devices and hosts be prone to attacks. Therefore, sending the ICMP Destination Unreachable packets has the following defects:

- The ICMP packets increase traffic volume and burden the network devices.
- If a device receives a large number of malicious attack packets and needs to return ICMP error packets, the device is busy handling ICMP packets, and the device performance is degraded.
- The ICMP Destination Unreachable packets indicate that the destination is unreachable. If there are malicious attacks, user terminals cannot normally use the network.

After you run the **icmp protocol-unreachable send** command, the device does not send ICMP Protocol Unreachable packets externally. This prevents the peer device from processing a large number of ICMP packets.

## Example

# Enable the function of sending ICMP Protocol Unreachable packets.

```
<HUAWEI> system-view
[HUAWEI] icmp protocol-unreachable send
```

# 6.9.23 icmp receive

## Function

The **icmp receive** command enables a switch to receive ICMP packets with the local IP address as the destination IP address.

The **undo icmp receive** command disables a switch from receiving ICMP packets with the local IP address as the destination IP address.

By default, switches are enabled to receive ICMP packets with the local IP address as the destination IP address.

## 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 packet. | The value is an integer ranging from 0 to 255. |
| **code** *icmp-code* | Specifies the code of an ICMP packet. | The value is an integer ranging from 0 to 255. |

| Parameter | Description | Value |
| --- | --- | --- |
| **name** *icmp-name* | Specifies the name of an ICMP packet. | The value is a string of case-insensitive characters, with spaces not supported. The value can be any of the following:<br>• echo<br>• echo-reply<br>• fragmentneed-dfset<br>• host-redirect<br>• host-tos-redirect<br>• host-unreachable<br>• information-reply<br>• information-request<br>• net-redirect<br>• net-tos-redirect<br>• net-unreachable<br>• parameter-problem<br>• port-unreachable<br>• protocol-unreachable<br>• reassembly-timeout<br>• source-quench<br>• source-route-failed<br>• timestamp-reply<br>• timestamp-request<br>• ttl-exceeded |
| **all** | Specifies all ICMP packets. | - |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

### Usage Scenario

- On secure networks, the device can normally receive ICMP packets. 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 use ICMP error packets to probe on the internal structure of the network.

To improve network performance or enhance security, run the **undo icmp receive** command to disable switches from receiving ICMP packets with the local IP address as the destination IP address.

After network performance improves, you can run the **icmp receive** command to enable switches to receive ICMP packets with the local IP address as the destination IP address.

**Precautions**

After the **undo icmp receive** command is run, the device no longer process ICMP packets of a certain type, causing the host to fail to ping the device.

## Example

# Disable the switch from receiving ICMP packets with the local IP address as the destination IP address whose type number is 3 and code number is 1.

```
<HUAWEI> system-view
[HUAWEI] undo icmp type 3 code 1 receive
```

# 6.9.24 icmp redirect send

## Function

The **icmp redirect send** command enables the switch to send ICMP redirect packets.

The **undo icmp redirect send** command disables the switch from sending ICMP redirect packets.

The function of sending ICMP Redirect packets is enabled.

## Format

**icmp redirect send**

**undo icmp redirect send**

## Parameters

None

## Views

Interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

ICMP error packets contain network information, such as network connectivity, host reachability, and route availability. ICMP error packets are ultimately returned to the sender because the sender is the logical receiver of the ICMP error packets. The sender learns about the error types from the ICMP error packets, and then determines how to retransmit the data.

ICMP Redirect packets are a type of ICMP error packets.

When a host starts, there may be only one default route to the gateway in its routing table. In the following situations, the device functions as a gateway to send an ICMP Redirect packet to the source host, requesting the host to select another next hop address for subsequent packet forwarding:

- The interface that receives the data packet is the same as the interface used to forward the packet.
- The device needs to forward a received packet. After looking up the routing table, the device finds that the next hop IP address is on the same network segment with the destination address of the packet.

After the device sends ICMP Redirect packets to the host that has only a few routes, the host can enrich the routing table and find out the optimal route.

The ICMP error packets facilitate network control and management. However, the inherent defects of the ICMP protocol make the routing devices and hosts be prone to attacks. Therefore, sending the ICMP error packets has the following defects:

- The ICMP packets increase traffic volume and burden the network devices.
- If a device receives a large number of malicious attack packets and needs to return ICMP error packets, the device is busy handling ICMP packets, and the device performance is degraded.
- The ICMP Redirect function increases the number of routes in the host's routing table. When many routes are added, the host performance will be degraded.

You need to decide whether to enable ICMP Redirect packet sending according to network situation.

**Precautions**

The command is used on the interface that receives ICMP packets.

## Example

# Enable VLANIF100 to send ICMP Redirect packets.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] icmp redirect send
```

# Enable GE0/0/1 to send ICMP Redirect packets.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] icmp redirect send
```

# 6.9.25 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 default format of ICMP Time Exceeded packets.

By default, ICMP Time Exceeded packets carry extension headers in compliant mode and original datagrams are of variable length.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

## 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

## 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
```

# 6.9.26 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 function of discarding ICMP packets with TTL values of 1 is disabled on the device.

**NOTE**

Only the S5720I-SI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

## Format

**icmp ttl-exceeded drop** { **slot** *slot-id* | **all** }

**undo icmp ttl-exceeded drop** { **slot** *slot-id* | **all** }

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **slot** *slot-id* | Indicates the slot ID. | The value is determined based on the device configuration. |
| **all** | Indicates all the devices. This parameter is used when you need to enable all the devices to discard or disable all the devices from discarding the ICMP packets whose TTL values are 1. | - |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

TTL is a field in an IP packet that limits the lifespan of the IP packet on the network. The TTL value is set by the sender, and is reduced by 1 every time the packet passes a device. If a forwarding device receives an IP packet of which the TTL is 0 and the destination address is not the local address, the device discards this packet and returns an ICMP packet to the sender.

ICMP packets are encapsulated into IP packets. When receiving an ICMP packet of which the destination address is not the local address and the TTL value is 1, the device discards the packet and returns an ICMP Time Exceeded.

When receiving a packet of which the TTL value is 1, the switch sends the packet to the CPU. The **tracert** function implements hop-by-hop detection using the packets with TTL value 1. If an attacker sends a large number of IP packets with TTL value 1 to a target device, the CPU of the target device is busy handling these IP packets and returns ICMP Destination Unreachable packets. Therefore, the CPU usage becomes high.

If a switch is configured to discard the ICMP packets with TTL value 1, the pressure on the switch can be reduced and network attacks can be prevented.

**Precautions**

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 slot 0
```

# 6.9.27 icmp ttl-exceeded send

## Function

The **icmp ttl-exceeded send** command enables an interface to send ICMP Time Exceeded packets.

The **undo icmp ttl-exceeded send** command disables an interface from sending ICMP Time Exceeded packets.

By default, an interface is enabled to send ICMP Time Exceeded packets.

## Format

**icmp ttl-exceeded send**

**undo icmp ttl-exceeded send**

## Parameters

None

## Views

Interface view

## Default Level

2: Configuration level

## Usage Guidelines

If the destination address of a received IP packet is not the local address and the TTL value is 1, a timeout error occurs. In this situation, the device discards the packet and returns an ICMP Time Exceeded packet to the source.

When replying with an ICMP Time Exceeded packet, an interface adds its IP address as the source IP address in the ICMP Time Exceeded packet, exposing the interface itself to attackers. In addition, after being attacked, the interface replies with numerous ICMP Time Exceeded packets, 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 packets.

## Example

# Enable VLANIF100 to send ICMP Time Exceeded packets.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] icmp ttl-exceeded send
```

# Enable GE0/0/1 to send ICMP Time Exceeded packets.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] icmp ttl-exceeded send
```

# 6.9.28 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.

**NOTE**

Only the S5720I-SI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

## Format

**icmp unreachable drop**

**undo icmp unreachable drop**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

ICMP error packets contain network information, such as network connectivity, host reachability, and route availability. ICMP error packets are ultimately returned to the sender because the sender is the logical receiver of the ICMP error packets. The sender learns about the error types from the ICMP error packets, and then determines how to retransmit the data.

The Destination Unreachable packets facilitate network control and management. However, the inherent defects of the ICMP protocol make the routing devices and

hosts be prone to attacks. Therefore, sending the ICMP Destination Unreachable packets has the following defects:

- The ICMP packets increase traffic volume and burden the network devices.
- If a device receives a large number of malicious attack packets and needs to return ICMP error packets, the device is busy handling ICMP packets, and the device performance is degraded.
- The ICMP Destination Unreachable packets indicate that the destination is unreachable. If there are malicious attacks, user terminals cannot normally use the network.

The switch sends ICMP Destination Unreachable packets to the CPU for processing. When a large number of such packets are received, the CPU may be overloaded. To reduce the number of ICMP packets on the network, you can enable the switch to discard ICMP Destination Unreachable packets. After the configuration, the workload on the switch is reduced and malicious attacks can be prevented.

## Example

# Enable the function of discarding ICMP Destination Unreachable packets.

```
<HUAWEI> system-view
[HUAWEI] icmp unreachable drop
```

# 6.9.29 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 function of discarding ICMP packets with TTL values of 1 is disabled on the device.

## Format

**icmp with-options drop** { **slot** *slot-id* | **all** }

**undo icmp with-options drop** { **slot** *slot-id* | **all** }

NOTE

Only the S5720I-SI, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, S5735S-S, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **slot** *slot-id* | The value is an integer. It must be the slot ID of the device that is inserted into the chassis. | The value is determined based on the device configuration. |
| **all** | Indicates all the stacking devices. This parameter is used when you need to enable all the devices to discard or disable all the devices from discarding the ICMP packets that carry options. | - |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

When the **ping -r** command is run to detect network connectivity, the IP packet is forwarded by Layer 3 routing devices. Every Layer 3 device fills its own IP address into the option field of the IP packet. When the IP packet reaches the destination, the ICMP Echo Reply packet should contain the IP addresses of all passing devices, including the devices on the forward and return paths. When the ping program receives the reply packet, it can display the IP addresses of all passing Layer 3 devices.

If the length of IP packet encapsulating the ICMP packet exceeds the interface MTU, this IP packet is fragmented. Only the IP header of the first fragment includes the option field. The fragment carrying the option field is sent to the protocol stack and processed by the CPU.

When malicious attacks are initiated using ICMP packets, the device needs to process a large number of fragments carrying the option field, so the forwarding performance of the device degrades. To reduce impact on the forwarding performance and prevent ICMP packet attacks, you can enable the device to discard the ICMP fragments carrying option fields.

## Example

# Enable the device to discard the ICMP packets that carry options.

```
<HUAWEI> system-view
[HUAWEI] icmp with-options drop slot 0
```

# 6.9.30 icmp-reply fast

## Function

The **icmp-reply fast** command enables the fast ICMP reply function.

The **undo icmp-reply fast** command disables the fast ICMP reply function.

By default, the fast ICMP reply function is enabled.

## Format

**icmp-reply fast**

**undo icmp-reply fast**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

The ping program is used to check network connectivity. If two hosts cannot ping each other, they cannot set up a connection. The ping program uses the ICMP protocol. It encapsulates ICMP Echo Request packets into IP packets, and sends the packets to the destination host. The destination host returns an ICMP Echo Reply packet to the source host. If the source host receives a reply within a certain period, the source host considers that the destination host is reachable.

In normal situations, after an interface receives an ICMP Echo Request packet, this packet is sent to the protocol stack and handled by the CPU.

After fast ICMP reply is enabled, if an interface receives an ICMP Echo Request packet of which the destination address is the local address, the packet is not sent to the protocol stack for handing by the CPU, but handled by the physical interface. This improves forwarding performance of the device.

**Precautions**

The fast ICMP reply function is not supported for fragmented packets, packets with IP options, and MPLS-encapsulated packets.

On the S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S, fast ICMP reply is not supported for packets whose TTL is 1.

A switch does not support fragmentation of the ICMP Echo Reply packets processed based on the fast ICMP reply mechanism to be sent to the remote end. The packets will not be discarded even if their length is greater than the MTU of the outbound interface.

For the S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6720S-S, S6735-S, S6720-EI, S6720S-EI:

- The fast ICMP reply function does not take effect on VBDIF interfaces.
- When a routed main interface (supporting Layer 2 and Layer 3 mode switching) is bound to a VPN instance, the fast ICMP reply function does not take effect on the interface.
- When a sub-interface is bound to a VPN instance, the fast ICMP reply function does not take effect on the interface.
- After VLAN mapping is configured, the VLANIF interface corresponding to the mapped VLAN does not support the fast ICMP reply function.

For the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, after fast ICMP reply is enabled, the ping detection cannot be blocked by the blacklist. This is because after the fast ICMP reply function is enabled, the ICMP Echo Request packets received on an interface of the device are not sent to the protocol stack or processed by the CPU. Instead, the interface directly processes the packets.

## Example

# Enable the fast ICMP reply function.

```
<HUAWEI> system-view
[HUAWEI] icmp-reply fast
```

# 6.9.31 ip error-packet-check disable

## Function

The **ip error-packet-check disable** command disables the IP packet checking function.

The **undo ip error-packet-check disable** command enables the IP packet checking function.

By default, the IP packet checking function is enabled.

**NOTE**

Only following model switches support this function:

S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S6720S-S, S5735S-H, S5736-S

## Format

**ip error-packet-check disable**

**undo ip error-packet-check disable**

## Parameters

None

## Views

Ethernet interface view, GE interface view, MultiGE interface view, XGE interface view, port group view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

When the link type of an interface is QinQ or the VLAN mapping or VLAN stacking function is configured on the interface, the system checks IP packets so that the device cannot transparently transmit IP error packets. In addition, during Layer 2 forwarding, devices cannot transparently transmit packets with the same source and destination IP addresses. To enable the device to transparently transmit IP error packets, you can run the **ip error-packet-check disable** command to disable the IP packet checking function.

**Precautions**

When the IP packet checking function is disabled, the IP subnet-based VLAN assignment, policy-based VLAN assignment, and IPv6 over IPv4 tunnel functions do not take effect. Therefore, confirm your action before disabling this function.

## Example

# Disable the IP packet checking function on the interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] ip error-packet-check disable
```

# 6.9.32 ip forward-broadcast

## Function

Using the **ip forward-broadcast** command, you can enable an interface to forward directed broadcast packets.

Using the **undo ip forward-broadcast** command, you can disable an interface from forwarding directed broadcast packets.

By default, disable the interface from forwarding directed broadcast packets.

## Format

**ip forward-broadcast** [ **acl** *acl-number* ]

**undo ip forward-broadcast**

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **acl** *acl-number* | Specifies the number of an ACL. | The value is an integer that ranges from 2000 to 3999.<br>• The number of a basic ACL ranges from 2000 to 2999.<br>• The number of an advanced ACL ranges from 3000 to 3999. |

## Views

VE sub-interface view, VBDIF interface view, VLANIF interface view, Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 25GE interface view, 40GE interface view, 100GE 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.

Hackers use directed broadcast packets to attack networks, which threatens the network security. Therefore, directed broadcast packets are isolated by Layer 3 switches in normal cases. However, in some scenarios, the device needs to receive or forward these directed broadcast packets. For example, when Wake on LAN (WOL) is configured on a PC, the command can be run to enable the interface to forward directed broadcast packets. (WOL enables a PC in dormancy or shutdown state to wake up from dormancy state to running state or turn from shutdown state to power-on state through the instruction from the peer of the network.)

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.

Only broadcast packets that match the permit action defined in the ACL are forwarded. Broadcast packets that match the deny action defined in the ACL or do not match any ACL rules are not forwarded.

**Precautions**

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.

This command does not apply to VPN scenarios, IP address unnumbered scenarios, and scenarios of conflicts between host routes and subnet broadcast routes due to network segment overlapping.

## Example

# Enable VLANIF100 to forward directed broadcast packets.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip forward-broadcast
```

# Enable GE0/0/1 to forward directed broadcast packets.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip forward-broadcast
```

# 6.9.33 ip forwarding converge normal

## Function

The **ip forwarding converge normal** command disables the device to perform Layer 2 forwarding for IP traffic during ring network switchover.

The **undo ip forwarding converge** command enables the device from performing Layer 2 forwarding for IP traffic during ring network switchover.

By default, the device is enabled from performing Layer 2 forwarding for IP traffic during ring network switchover.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

## Format

**ip forwarding converge normal**

**undo ip forwarding converge**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

When the device deployed with the ring network protocols (STP, RSTP, MSTP, SEP, ERPS, RRPP, VBST, and Smart Link) performs link switchover due to a link fault, the ARP entries need to be learned again. This deteriorates the Layer 3 convergence performance of IP traffic. If the device is enabled to perform Layer 2 forwarding for IP traffic during the switchover, the convergence performance can be improved. By default, the device is enabled from performing Layer 2 forwarding for IP traffic during ring network switchover.

**Precautions**

After the device is enabled to perform Layer 2 forwarding for IP traffic, it will forward the IP traffic in broadcast mode during ring network switchover. Therefore, the IP traffic increases within a short time.

## Example

# Disable the device from performing Layer 2 forwarding for IP traffic during ring network switchover.

```
<HUAWEI> system-view
[HUAWEI] ip forwarding converge normal
```

# 6.9.34 ip forwarding disable

## Function

The **ip forwarding disable** command disables IPv4 Layer 3 unicast forwarding on a switch.

The **undo ip forwarding disable** command enables IPv4 Layer 3 unicast forwarding on a switch.

By default, IPv4 Layer 3 unicast forwarding is enabled on a switch.

## Format

**ip forwarding disable**

**undo ip forwarding disable**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

You can run this command to disable IPv4 Layer 3 unicast forwarding on a switch.

After IPv4 Layer 3 unicast forwarding is disabled on a switch, the IPv4 routing function becomes ineffective on the switch, and the switch cannot forward Layer 3 packets based on the IPv4 routing table and FIB table.

**Precautions**

Running this command on a switch disables IPv4 Layer 3 packet forwarding at the hardware layer and CPU software layer.

## Example

# Disable IPv4 Layer 3 unicast forwarding on the switch.

```
<HUAWEI> system-view
[HUAWEI] ip forwarding disable
Warning: This operation will close IPv4 forwarding function and affect IPv4 traffic forwarding. Continue?
[Y/N]:y
```

# 6.9.35 ip ttl-expired drop

## Function

The **ip ttl-expired drop** command enables the switch to discard IP packets with expired TTL.

The **undo ip ttl-expired drop** command disables the switch from discarding IP packets with expired TTL.

By default, the function of discarding IP packets with expired TTL is disabled.

## Format

**ip ttl-expired drop**

**undo ip ttl-expired drop**

NOTE

Only the S5720I-SI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

TTL is a field in an IP packet that limits the lifespan of the IP packet on the network. The TTL value is set by the sender, and is reduced by 1 every time the packet passes a device. If a forwarding device receives an IP packet of which the TTL is 0 and the destination address is not the local address, the device discards this packet.

If a device receives many IP packets with TTL value 1, the device may undergo an attack. Run the **ip ttl-expired drop** command to enable the device to discard the IP packets with expired TTL. Then the device discards the packets with TTL value 1, but does not send them to the CPU.

**Precautions**

After the **ip ttl-expired drop** command is run, some packets that have the TTL value 1 but need to be processed by the CPU are also discarded. Therefore, after the attack is removed, run the **undo ip ttl-expired drop** command to disable the device from discarding the IP packets with expired TTL.

## Example

# Enable the switch to discard IP packets with expired TTL.

```
<HUAWEI> system-view
[HUAWEI] ip ttl-expired drop
```

# 6.9.36 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.

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

Configuring source IP address verification enables an interface to check validity of source IP addresses of received packets. Packets with invalid addresses are discarded, which improves the network security.

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 checks validity of source IP addresses of the packets that need to be 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.

If the mask in the IP address of the received packet is of 31 bits, the receiver considers it as a valid source address without checking the broadcast address of the subnet.

Run the **display this** command in the interface view to check configuration of checking validity of source IP addresses.

## Example

# Enable VLANIF100 to check validity of source IP addresses of received packets.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip verify source-address
```

# Enable GE0/0/1 to check validity of source IP addresses of received packets.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ip verify source-address
```

# 6.9.37 ipv4 destination-unreachable drop

## Function

The **ipv4 destination-unreachable drop** command enables the function of discarding IP packets that match no routing entry.

The **undo ipv4 destination-unreachable drop** command disables the function of discarding IP packets that match no routing entry.

By default, the function of discarding IP packets that match no routing entry is enabled.

## Format

**ipv4 destination-unreachable drop**

**undo ipv4 destination-unreachable drop**

NOTE

Only the S5720I-SI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

### Usage Scenario

If the switch receives an IP packet that matches no routing entry in the local routing table, it sends the packet to the CPU. If a lot of IP packets match no

routing entry because of an attack or incorrect network configuration, the CPU is busy. To prevent this problem, run the **ipv4 destination-unreachable drop** command to configure the switch to discard these packets.

**Precautions**

If you run the **ipv4 destination-unreachable drop** command, the switch does not respond to ICMP error packets when a route fails to match the routing policies. To enable the switch to respond to these ICMP packets, you need to run the **undo ipv4 destination-unreachable drop** command.

On the S6720-EI, S6735-S, and S6720S-EI, when both the **ipv4 destination-unreachable drop** command and the traffic policy command are run, both the drop action and the redirection action take effect. The ICMP redirection packets are discarded because the drop action has a higher priority than the redirection action. This leads to a redirection failure for ICMP packets. To make the redirection action for ICMP packets effective, run the **undo ipv4 destination-unreachable drop** command to disable the drop action. However, disabling the drop action will degrade the attack defense performance of the system. You must configure the two actions properly according to the network requirements.

For the S6720-EI, S6735-S and S6720S-EI, if the resource allocation mode is set to **enhanced-ipv4** or **ipv4-ipv6 6:1** using the **assign resource-mode** command, the **ipv4 destination-unreachable drop** command does not take effect.

## Example

# Enable the function of discarding IP packets that match no routing entry.

```
<HUAWEI> system-view
[HUAWEI] ipv4 destination-unreachable drop
```

# 6.9.38 ipv4 fragment enable

## Function

The **ipv4 fragment enable** command enables fragmentation for outgoing forwarding-plain IP packets.

The **undo ipv4 fragment enable** command disables fragmentation for outgoing forwarding-plain IP packets.

By default, fragmentation for outgoing forwarding-plain IP packets is disabled.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

## Format

**ipv4 fragment enable**

**undo ipv4 fragment enable**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

By default, only packets on the control plane can be fragmented according to the MTU on an interface. Packets on the forwarding plane can be forwarded normally without limited by the MTU. When the remote device or intermediate forwarding device receives IP packets, if it checks the packet length and discards packets whose length is longer than the MTU on the interface, network communication is interrupted. For the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, you can run the **ipv4 fragment enable** command to enable fragmentation for outgoing forwarding-plane IP packets so that packets on the forwarding plane are fragmented based on the MTU on the interface.

**Precautions**

Before configuring the **ipv4 fragment enable** command, set a proper MTU. If the MTU is small, there may be many fragments of IP packets, causing the Layer 3 forwarding performance of IP packets to deteriorate.

## Example

# Enable fragmentation for outgoing IP packets.

```
<HUAWEI> system-view
[HUAWEI] ipv4 fragment enable
```

# 6.9.39 ipv6 destination-unreachable drop

## Function

The **ipv6 destination-unreachable drop** command enables the switch to discard the packets that do not match IPv6 routing entries.

The **undo ipv6 destination-unreachable drop** command disables the switch from discarding the packets that do not match IPv6 routing entries.

By default, the device discards the packets that do not match IPv6 routing entries.

## Format

**ipv6 destination-unreachable drop**

**undo ipv6 destination-unreachable drop**

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

Generally, the device sends the IPv6 packets that do not match routing entries to the CPU for processing. If many IPv6 packets do not match routing entries because of an attack or improper network configurations, the CPU is busy. To prevent this situation, run the **ipv6 destination-unreachable drop** command to configure the switch to discard these packets.

**Precautions**

If the **ipv6 destination-unreachable drop** command is used and a traffic policy with the redirect action is configured, both the drop action and the redirect action take effect. Because the drop action has a higher priority than the redirect action, ICMPv6 Redirect packets are discarded. This leads to a redirection failure. To make the redirect action take effect, run the **undo ipv6 destination-unreachable drop** command to disable the drop action. However, disabling the drop action will degrade the attack defense performance of the system. You must configure the two actions properly according to network requirements.

After the **ipv6 destination-unreachable drop** command is used, the switch does not respond to the ICMPv6 Error packets caused when IPv6 packets do not match routing entries until the drop action is disabled.

For the S6720-EI, S6735-S and S6720S-EI, if the resource allocation mode is set to **enhanced-ipv4** or **ipv4-ipv6 6:1** using the **assign resource-mode** command, the **ipv6 destination-unreachable drop** command does not take effect.

## Example

# Configure the switch to discard the packets that do not match IPv6 routing entries.

```
<HUAWEI> system-view
[HUAWEI] undo ipv6 destination-unreachable drop
```

# 6.9.40 ipv6 with-options drop

## Function

The **ipv6 with-options drop** command enables the switch to discard IPv6 packets destined for the switch and containing specified extension headers.

The **undo ipv6 with-options drop** command disables the switch from discarding IPv6 packets destined for the switch and containing specified extension headers.

By default, the switch is disabled from discarding IPv6 packets destined for the switch and containing specified extension headers.

## Format

**ipv6 with-options drop**

**undo ipv6 with-options drop**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

IPv6 packets may contain the following extension headers:

- Routing header: An IPv6 source node uses this header to specify the intermediate nodes that a packet must pass through on the way to its destination.
- Fragment header: The length of IPv6 packets to be forwarded cannot exceed the maximum transmission unit (MTU) specified on interfaces of devices along the forwarding path. When the packet length exceeds the MTU, the packet needs to be fragmented. In IPv6, the fragment header is used by an IPv6 source node to send a packet larger than the MTU. Fragmentation in IPv6 is performed only by source nodes, not by intermediate nodes along the path a packet traverses.
- Destination options header: This header carries information that only the destination node of a packet processes.

Malicious attacks can be initiated using these IPv6 extension headers. For example, the routing header can be used to specify a node that packets must pass through. The fragment header can be used to set the MTU to a small value on the source node, leading to a large number of data fragments. The destination options header can specify destination devices to process IPv6 packets. If attackers send a large number of such IPv6 packets to the switch, the switch is busy handling these

packets, degrading the forwarding performance. To prevent malicious network attacks and reduce impact on the forwarding performance, you can enable the switch to discard IPv6 packets destined for the switch and containing specified extension headers.

## Example

# Enable the switch to discard IPv6 packets destined for the switch and containing specified extension headers.

```
<HUAWEI> system-view
[HUAWEI] ipv6 with-options drop
```

# 6.9.41 load-balance (system view)

## Function

The **load-balance** command configures a load balancing mode for public IP packet forwarding.

The **undo load-balance** command restores the load balancing mode for public IP packet forwarding to the default configuration.

By default, flow-based load balancing is used for public IP packet forwarding

## Format

**load-balance** { **flow** | **packet** } [ **all** | **slot** *slot-id* ]

**undo load-balance packet** [ **all** | **slot** *slot-id* ]

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **flow** | Indicates flow-based load balancing. | - |
| **packet** | Indicates packet-based load balancing. | - |
| **all** | In a stack, the configuration is applied to all devices in the stack. On a stand-alone switch, the configuration is applied to the local device. | - |
| **slot** *slot-id* | Indicates that the configuration is applied to the device with the specified stack ID. | The value is an integer. It has a fixed value of 0 in a non-stack scenario, and depends on the device configuration in a stack scenario. |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Scenario**

If flow-based load balancing is used, the hash algorithm is used to calculate a value for selecting a link to forward packets. The value is calculated based on the protocol type, source IP address, destination IP address, source port number, and destination port number.

If packet-based load balancing is used, packets are forwarded through different links. Packet-based load balancing can be implemented only for packets forwarded by the CPU such as protocol packets.

**Precautions**

The **load-balance** command takes effect on packets delivered by the local device and IP/MPLS packets processed by the CPU.

## Example

# Configure packet-based load balancing for public IP packet forwarding.

```
<HUAWEI> system-view
[HUAWEI] load-balance packet
```

# 6.9.42 load-balance vpn

## Function

The **load-balance vpn** command configures a load balancing mode for private IP packet forwarding.

The **undo load-balance vpn** command restores the load balancing mode for private IP packet forwarding to the default configuration.

By default, packet-based load balancing is used for private IP packet forwarding

## Format

**load-balance** { **flow** | **packet** } **vpn**

**undo load-balance flow vpn**

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **flow** | Indicates flow-based load balancing. | - |
| **packet** | Indicates packet-based load balancing. | - |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Scenario**

If flow-based load balancing is used, the hash algorithm is used to calculate a value for selecting a link to forward packets. The value is calculated based on the protocol type, source IP address, destination IP address, source port number, and destination port number.

If packet-based load balancing is used, packets are forwarded through different links. Packet-based load balancing can be implemented only for packets forwarded by the CPU such as protocol packets.

**Precautions**

The **load-balance vpn** command takes effect on packets delivered by the local device and IP/MPLS packets processed by the CPU.

## Example

# Configure flow-based load balancing for private IP packet forwarding.

```
<HUAWEI> system-view
[HUAWEI] load-balance flow vpn
```

# 6.9.43 management-port icmp-reply fast disable

## Function

The **management-port icmp-reply fast disable** command disables the fast ICMP reply function on the management Ethernet port.

The **undo management-port icmp-reply fast disable** command enables the fast ICMP reply function on the management Ethernet port.

By default, the fast ICMP reply function is enabled on the management Ethernet port.

NOTE

The following models support this command: S5731-H, S5731S-H, S5731-S, S5731S-S, S5732-H, S5735-S, S5735-S-I, S5735S-H, S5735-L, S5736-S, S6730-H, S6730S-H, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-S, S6720S-EI.

## Format

**management-port icmp-reply fast disable**

**undo management-port icmp-reply fast disable**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

The ping program is used to check network connectivity. If two hosts cannot ping each other, they cannot set up a connection. The ping program uses the ICMP protocol. It encapsulates ICMP Echo Request packets into IP packets, and sends the packets to the destination host. The destination host returns an ICMP Echo Reply packet to the source host. If the source host receives a reply within a certain period, the source host considers that the destination host is reachable.

In normal situations, after the management Ethernet port of a device receives an ICMP Echo Request packet, this packet is sent to the protocol stack and handled by the CPU.

After fast ICMP reply is enabled, if the management Ethernet port receives an ICMP Echo Request packet of which the destination address is the local address, the packet is not sent to the protocol stack for handing by the CPU, but handled by the management Ethernet port. This improves forwarding performance of the device.

**Precautions**

The fast ICMP reply function is not supported for fragmented packets, packets with IP options, and MPLS-encapsulated packets.

## Example

# Enable the fast ICMP reply function on the management Ethernet port.

```
<HUAWEI> system-view
[HUAWEI] undo management-port icmp-reply fast disable
```

# 6.9.44 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

A socket monitor monitors and records each connection. A RawLink monitor also monitors interfaces. The socket monitor records specific protocol events that occur during operations and logs information in the disk space.

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
```

# 6.9.45 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
```

# 6.9.46 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* ]

## 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
```

# Clear IP statistics on VLANIF10.

```
<HUAWEI> reset ip statistics interface vlanif 10
```

## 6.9.47 reset rawip statistics

### Function

The **reset rawip statistics** command clears RawIP packet statistics.

### Format

**reset rawip statistics**

### Parameters

None

### Views

User view

### Default Level

3: Management level

### Usage Guidelines

You need to clear the existing statistics about RawIP packets before using the **display rawip statistics** command to view the statistics about RawIP packets in a specified period.

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
```

# 6.9.48 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

### Usage Scenario

To delete TCP packet statistics, run the **reset tcp statistics** command. To view TCP packet statistics, run the **display tcp statistics** [ **verbose** ] command. The command output contains the number of sent packets, the number of received packets, or the number of TCP packets for each protocol (verbose). You can run the **reset tcp statistics** command to delete existing statistics and then run the **display tcp statistics** command to collect statistics. The statistics help you check whether TCP packet counts are correct or help you diagnose faults.

### Precautions

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
```

# 6.9.49 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

**Usage Scenario**

To delete UDP packet statistics, run the **reset udp statistics** command. To view UDP packet statistics, run the **display udp statistics** [ **verbose** ] command. The command output contains the number of sent packets, the number of received packets, or the number of UDP packets for each protocol (verbose). You can run the **reset udp statistics** command to delete existing statistics and then run the **display udp statistics** command to collect statistics. The statistics help you check whether UDP packet counts are correct or help you diagnose faults.

**Precautions**

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
```

# 6.9.50 set priority

## Function

The **set priority** command sets the 802.1p priority or DSCP priority of packets.

The **undo set priority** command cancels the settings of the 802.1p priority or DSCP priority of packets.

By default, the 802.1p priority or DSCP priority of packets is not set.

## Format

**set priority 8021p** *8021p-number*

**undo set priority 8021p**

**set priority dscp** *dscp-number* [ **if-match acl** *acl-number* ]

**undo set priority dscp** [ **if-match acl** *acl-number* ]

NOTE

Only the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support **if-match acl** *acl-number*.

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **8021p** *8021p-number* | Specifies the 802.1p priority of packets. | The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority. |
| **dscp** *dscp-number* | Specifies the DSCP priority of packets. This parameter takes effect only for IPv4 packets. | The value is an integer that ranges from 0 to 63. |
| **if-match acl** *acl-number* | Specifies the number of an ACL. | The value is an integer that ranges from 3000 to 3999. |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

### Usage Scenario

You can run the **set priority** command to set the 802.1p priority or DSCP priority of packets sent by the switch.

To change the DSCP priority of protocol packets that meet specified characteristics and are sent by the switch, you can use an ACL to match these packets.

### Precautions

This command takes effect only for IPv4 but not for IPv6.

If the packet priority has been specified in the protocol, the **set priority 8021p** command does not take effect.

If you use ACLs to match packets whose DSCP priority is to be changed, you can specify up to eight ACLs, each of which supports a maximum of 32 rules. The following fields can be matched:

- ICMP packets: source IP address, destination IP address, protocol number, icmp-type, icmp-code, fragment, precedence, tos, dscp, ttl-expired, vpn-instance, and time-range
- TCP packets: source IP address, destination IP address, protocol number, source port, destination port, tcp-flag, fragment, precedence, tos, dscp, ttl-expired, vpn-instance, and time-range
- UDP packets: source IP address, destination IP address, protocol number, source port, destination port, fragment, precedence, tos, dscp, ttl-expired, vpn-instance, and time-range
- Other protocol packets: source IP address, destination IP address, protocol number, fragment, precedence, tos, dscp, ttl-expired, vpn-instance, and time-range

The switch cannot use ACL-based matching to change the DSCP priority of the following protocol packets:

- Protocol packets that are not sent from the protocol stack, such as fast ICMP reply packets and NetStream packets
- Protocol packets whose priority can be configured using a command (for example, you can run the **tos** command to set the priority of NQA packets)

## Example

# Set the DSCP priority to 10.

```
<HUAWEI> system-view
[HUAWEI] set priority dscp 10
```

# 6.9.51 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**

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *mss-value* | Specifies the minimum MSS value for a TCP connection. | The value ranges from 32 bytes 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**

The minimum MSS value configured using this command is not the negotiation parameter value carried in the MSS option. The negotiation parameter value carried in the MSS option of packets sent by the local device is calculated based on the MTU value.

The minimum MSS value configured using the **tcp min-mss** command must be less than the maximum MSS value configured using the **tcp max-mss** command.

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
```

# 6.9.52 tcp max-mss

## Function

The **tcp max-mss** command configures the maximum Maximum Segment Size (MSS) value for a TCP connection.

The **undo tcp max-mss** command deletes the maximum MSS value of a TCP connection.

By default, the maximum MSS value is not configured for TCP connections.

## Format

**tcp max-mss** *mss-value*

**undo tcp max-mss**

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *mss-value* | Specifies the maximum MSS value for a TCP 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 TCP connection, the MSS value is negotiated, which indicates the maximum length of packets that the local device can receive. This length is the TCP payload length, excluding that of the TCP header. If the path MTU is unavailable on one end of a TCP connection, this end cannot adjust the TCP packet size based on the MTU. As a result, this end may send TCP packets that are longer than the MTUs on intermediate devices, which will discard these packets. To prevent this problem, run the **tcp max-mss** command on either end of a TCP connection to set the maximum MSS value of TCP packets. Then the MSS value negotiated by both ends will not exceed this maximum MSS value, and accordingly TCP 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 max-mss** command must be greater than the minimum MSS value configured using the **tcp min-mss** command.

## Example

# Set the maximum MSS value for a TCP connection to 1024 bytes.

```
<HUAWEI> system-view
[HUAWEI] tcp max-mss 1024
```

# 6.9.53 tcp send-trap bind-port

## Function

The **tcp send-trap bind-port** command configures a TCP port number list.

The **undo tcp send-trap bind-port** command restores the default TCP port number list.

By default, no TCP port number list is configured.

## Format

**tcp send-trap bind-port** { *port-number* } &<1-10>

**undo tcp send-trap bind-port** { { *port-number* } &<1-10> | **all** }

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *port-number* | Specifies a TCP port number. | The value is an integer in the range from 1 to 65535. |
| **all** | Indicates all TCP port numbers in a TCP port number list. | - |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

If you need to pay special attention to some TCP port numbers, you can run this command to add them to a TCP port number list. If port numbers in a TCP port number list are bound to services or an attempt is made to bind such numbers to services, the device sends an event alarm so that you can monitor the TCP port numbers.

**Precautions**

When the **undo tcp send-trap bind-port all** command is run, the system prompts you for confirmation.

## Example

# Configure a TCP port number list.

```
<HUAWEI> system-view
[HUAWEI] tcp send-trap bind-port 20 21 23 80
```

# 6.9.54 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. The default value is 675s. |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

When a TCP connection changes from FIN_WAIT_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
```

## 6.9.55 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. |

### 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
```

## 6.9.56 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**

### 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
```

# 6.10 Basic IPv6 Configuration Commands

## 6.10.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

## 6.10.2 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**

### Parameters

None

### Views

All views

### Default Level

1: Monitoring level

### Usage Guidelines

The **display default-parameter tcp6** command displays the default values of all configurable parameters on the TCP6 module.

### 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 6-56** Description of the display default-parameter tcp6 command output

| Item | Description |
| --- | --- |
| SYN Timeout Value(sec) | TCP SYN-Wait timer value.<br>To configure this parameter, run the **tcp ipv6 timer syn-timeout** command. |
| FIN Timeout Value(sec) | TCP FIN-Wait timer value.<br>To configure this parameter, run the **tcp ipv6 timer fin-timeout** command. |
| Window Size(KBytes) | TCP6 slide window size.<br>To configure this parameter, run the **tcp ipv6 window** command. |

# 6.10.3 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* | Indicates the ICMPv6 traffic statistics on the specified interface. | - |

## 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.

```
<HUAWEI> display icmpv6 statistics interface vlanif 100
ICMPv6 protocol:

 Sent packets:
   Total              : 2
   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   : 1
   Neighbor advert    : 1          Redirected         : 0
   Rate limited       : 0          Cert path advert   : 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          Cert path solicit  : 0
```

**Table 6-57** 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. |

| Item | Description |
| --- | --- |
| 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. |
| 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. |
| Cert path advert | Total number of sent CPS packets. This parameter is not supported currently and displayed as 0. |
| 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. |

| Item | Description |
| --- | --- |
| 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. |
| 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. |
| Cert path solicit | Total number of received CPA packets. This parameter is not supported currently and displayed as 0. |

## 6.10.4 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 the device suffers from overlapping fragment attacks, the administrator can run 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. The administrator can take proper actions on the attack source.

## Example

# Display source information about overlapping fragment attacks.

```
<HUAWEI> display ipv6 attack-source overlapping-fragment
Attack-source overlapping fragment table:

------------------------------------------------------------------------------
 Source IP          : FC00::1
 Destination IP     : FC00::2
 Interface name     : Vlanif2
 VPN name           :
 VLAN               : 0                          CEVLAN: 0
 Attacked time      : 2011-09-29 01:01:28
------------------------------------------------------------------------------

Total: 1
```

**Table 6-58** 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. |

# 6.10.5 display ipv6 interface

## Function

The **display ipv6 interface** command displays IPv6 information on an interface.

## Format

**display ipv6 interface** [ *interface-type interface-number* | **brief** ]

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *interface-type interface-number* | Displays IPv6 information on a specified interface.<br>• *interface-type* specifies the interface type.<br>• *interface-number* specifies the interface number.<br>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 VLANIF 2.

```
<HUAWEI> display ipv6 interface vlanif 2
Vlanif2 current state : DOWN
IPv6 protocol current state : DOWN
IPv6 is enabled, link-local address is FE80::200:1FF:FE04:5D00 [TENTATIVE]
  Global unicast address(es):
    FC00::1, subnet is FC00::/64 [TENTATIVE]
  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
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisement max interval 600 seconds, min interval 200 seconds
ND router advertisements live for 1800 seconds
ND router advertisements hop-limit 64
ND default router preference medium
Hosts use stateless autoconfig for addresses
```

**Table 6-59** Description of the **display ipv6 interface** command output

| Item | Description |
| --- | --- |
| Vlanif2 current state | Current physical status of VLANIF 2.<br>• UP: enabled<br>• DOWN: disabled |
| IPv6 protocol current state | Current protocol status of the interface.<br>• UP: enabled<br>• DOWN: disabled |
| IPv6 is enabled | IPv6 is enabled. |
| link-local address | Link-local address on the interface.<br>After an IPv6 address is configured on the interface, the system automatically assigns a link-local address for the interface. To manually 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.<br>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. |
| TENTATIVE | When the interface is in DOWN state, the IPv6 address is TENTATIVE. |
| MTU | MTU of the interface.<br>To configure the MTU for an interface, run the **ipv6 mtu** command. |
| ND DAD is enabled | NS packets are sent when the system performs Duplicate Address Detection (DAD). |

| Item | Description |
| --- | --- |
| number of DAD attempts | Number of times duplicate address detection is performed. |
| ND reachable time | Neighbor reachable time. |
| ND retransmit interval | Retransmission interval of NS packets. |
| ND stale time | Aging time of ND entries in STALE state. |
| ND advertised reachable time | Reachable time of NA packets.<br>**NOTE**<br>This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface. |
| ND advertised retransmit interval | Retransmission interval of NA packets.<br>**NOTE**<br>This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface. |
| ND router advertisement max interval 600 seconds, min interval 200 seconds | Maximum and minimum interval of RA packets.<br>**NOTE**<br>This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface. |
| ND router advertisements live for | Router lifetime in RA packets.<br>**NOTE**<br>This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface. |
| ND router advertisements hop-limit | Hop limit of RA packets.<br>**NOTE**<br>This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface. |
| ND default router preference | Default route priority in RA packets.<br>**NOTE**<br>This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface. |
| Hosts use stateless autoconfig for addresses | Hosts obtain IPv6 addresses by means of stateless auto-configuration.<br>**NOTE**<br>This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface. |

# Display brief IPv6 information about all interfaces.

```
<HUAWEI> display ipv6 interface brief
*down: administratively down
(l): loopback
(s): spoofing
Interface                  Physical            Protocol
LoopBack0                  up                  up(s)
[IPv6 Address] Unassigned
Vlanif2                    down                down
[IPv6 Address] 2001:db8:1::1 [TENTATIVE]
```

**Table 6-60** Description of the **display ipv6 interface brief** command output

| Item | Description |
| --- | --- |
| *down | Reason that interface is physically Down. **administratively down** indicates that the network administrator has executed the **shutdown (interface view)** command on the interface. |
| (l) | This interface is enabled with the loopback function. |
| (s) | This interface is enabled with the spoofing function. |
| Interface | Name of an interface. |
| Physical | Physical status of the interface. |
| Protocol | Link layer protocol status of the interface. |
| IPv6 Address | IPv6 address configured for the interface. If no IPv6 address is assigned to the interface, this field displays Unassigned. |
| TENTATIVE | When the interface is in Down state, the IPv6 address is TENTATIVE. |

# 6.10.6 display ipv6 interface tunnel

## Function

The **display ipv6 interface tunnel** command displays IPv6 information on a tunnel interface.

NOTE

Only the S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

## Format

**display ipv6 interface tunnel** *interface-number*

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *interface-number* | Displays the tunnel interface number. | - |

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

The **display ipv6 interface tunnel** command displays IPv6 information on a tunnel interface.

## Example

# Display IPv6 information on Tunnel1.

```
<HUAWEI> display ipv6 interface tunnel 1
Tunnel1 current state : UP
IPv6 protocol current state : DOWN
IPv6 is enabled, link-local address is FE80::2E0:9FF:FE87:7890 [TENTATIVE]
  Global unicast address(es):
    FC00:1::1, subnet is FC00:1::/64 [TENTATIVE]
  Joined group address(es):
    FF02::1:FF87:7890
    FF02::1:FF00:1
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND stale time is 1200 seconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisement max interval 600 seconds, min interval 200 seconds
  ND router advertisements live for 1800 seconds
  ND router advertisements hop-limit 64
  ND default router preference medium
  Hosts use stateless autoconfig for addresses
```

**Table 6-61** Description of the **display ipv6 interface tunnel** command output

| Item | Description |
| --- | --- |
| Tunnel1 current state | Current status of the tunnel interface:<br>• UP: enabled<br>• DOWN: disabled<br>When working properly, an IPv6 over IPv4 tunnel is in Up state. |

| Item | Description |
| --- | --- |
| IPv6 protocol current state | Current status of the link layer protocol:<br>• UP: enabled<br>• DOWN: disabled<br>When working properly, an IPv6 over IPv4 tunnel is in Up state. |
| IPv6 is enabled | IPv6 is enabled. |
| link-local address | Link-local address on the interface.<br>After an IPv6 address is configured on the interface, the system automatically assigns a link-local address for the interface. To manually configure a link-local address for an interface, run the **ipv6 address link-local** command. |
| Global unicast address(es) | IPv6 global unicast address.<br>To configure an IPv6 global unicast address, run the **ipv6 address** command. |
| Joined group address(es) | Addresses of multicast groups that the interface joins. |
| TENTATIVE | When the interface is in DOWN state, the IPv6 address is TENTATIVE. |
| MTU | MTU of the interface.<br>To configure the MTU of the interface, run the **ipv6 mtu** command. |
| ND reachable time | Reachable time of ND packets. |
| ND retransmit interval | Interval for retransmitting ND packets. |
| ND stale time | Time period for the neighbor to keep the STALE state. |
| ND advertised reachable time | Reachable time of NA packets.<br>**NOTE**<br>This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface. |
| ND advertised retransmit interval | Retransmission interval of NA packets.<br>**NOTE**<br>This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface. |

| Item | Description |
| --- | --- |
| ND router advertisement max interval 600 seconds, min interval 200 seconds | Maximum and minimum interval of RA packets.<br>**NOTE**<br>This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface. |
| ND router advertisements live for | Router lifetime in RA packets.<br>**NOTE**<br>This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface. |
| ND router advertisements hop-limit | Hop limit of RA packets.<br>**NOTE**<br>This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface. |
| ND default router preference | Default route priority in RA packets.<br>**NOTE**<br>This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface. |
| Hosts use stateless autoconfig for addresses | Hosts obtain IPv6 addresses by means of stateless auto-configuration.<br>**NOTE**<br>This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface. |

# 6.10.7 display ipv6 nd track

## Function

The **display ipv6 nd track** command displays information about the changes in the outbound interfaces of ND entries on VLANIF interfaces.

## Format

**display ipv6 nd track**

## Parameters

None

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

### Usage Scenario

If the outbound interfaces of ND entries learned by a VLANIF interface change, traffic is intermittently interrupted. To keep track of the outbound interface changes, run the **display ipv6 nd track** command to display the change time.

### Prerequisites

A VLANIF interface has ND entries, and their outbound interfaces have changed.

### Precautions

After the **display ipv6 nd track** command is run, the following types of changes are displayed:

- The outbound interface of a dynamic ND entry learned by the VLANIF interface changes to another interface.
- The outbound interface of a static ND entry configured on the VLANIF interface is changed to another interface.
- A dynamic or static ND entry on the VLANIF interface is deleted.

The following types of changes are not displayed:

- ND entries on a non-VLANIF interface change.
- A new ND entry is learned.
- A new static ND entry is configured.

## Example

# Display information about the changes in the outbound interfaces of ND entries on VLANIF interfaces.

```
<HUAWEI> display ipv6 nd track
Operate Flag : Modify
IPv6-Address : 2001:db8::1
MAC-Address  : 00e0-fc12-3456
VLAN         : 1000
Old-Port     : GE0/0/1
New-Port     : GE0/0/11
System-Time  : 2017-10-19 12:10:12

Operate Flag : Modify
IPv6-Address : 2001:db8:2::2
MAC-Address  : 00e0-fc12-3456
VLAN         : 1000
Old-Port     : GE0/0/1
New-Port     : GE0/0/11
System-Time  : 2017-09-19 12:13:12

Operate Flag : Delete
IPv6-Address : 2001:db8:3::3
MAC-Address  : 00e0-fc12-3455
VLAN         : 300
Old-Port     : GE0/0/2
New-Port     :
System-Time  : 2017-08-19 12:12:12
```

**Table 6-62** Description of the **display ipv6 nd track** command output

| Item | Description |
| --- | --- |
| Operate Flag | Operation flag.<br>• Modify: indicates that the outbound interface changes.<br>• Delete: indicates that the ND entry is deleted. |
| IPv6-Address | IPv6 address of the ND entry. |
| MAC-Address | MAC address of the ND entry. |
| VLAN | VLAN ID of the VLANIF interface. |
| Old-Port | Original outbound interface of the ND entry. |
| New-Port | New outbound interface of the ND entry. |
| System-Time | Time when the outbound interface changed. |

# 6.10.8 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* ] ] ]

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **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. |

| Parameter | Description | Value |
| --- | --- | --- |
| **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. | - |
| **vpn-instance** *vpn-instance-name* | Displays neighbor entries of a specified VPN instance. | The value must be an existing VPN instance name. |
| **cevid** *cevid* | Specifies the inner tag. | 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* [ **cevid** *cevid* ] ] ] command.
- To view the neighbor entry on a sub-interface for QinQ VLAN tag termination or Dot1q VLAN tag termination, 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 of IPv6 address FC00::2.

```
<HUAWEI> display ipv6 neighbors fc00::2
------------------------------------------------------------------------------
IPv6 Address : FC00::2
Link-layer   : 00e0-fc89-fe6e          State : STALE
Interface    : GE0/0/1                 Age   : 00h19m12s
VLAN         : -                     CEVLAN: -
VPN name     :                         Is Router: FALSE
------------------------------------------------------------------------------
Total: 1        Dynamic: 1         Static: 0
```

# Display neighbor entries on a specified interface.

```
<HUAWEI> display ipv6 neighbors vlanif 11
------------------------------------------------------------------------------
IPv6 Address : FC00::3
Link-layer   : 0001-0001-0012                State : INCMP
Interface    : GE0/0/1                       Age   : 00h19m12s
VLAN         : 11                          CEVLAN: -
VPN name     : v1                            Is Router: TRUE

------------------------------------------------------------------------------
Total: 1       Dynamic: 0       Static: 1
```

# View the neighbor entries on the QinQ termination sub-interface GE0/0/1.1.

```
<HUAWEI> display ipv6 neighbors gigabitethernet 0/0/1.1 vid 1 cevid 1
------------------------------------------------------------------------------
IPv6 Address : 2001:db8::2
Link-layer   : 00e0-3602-8100                State : REACH
Interface    : GE0/0/1.1                     Age   : -
VLAN         : 1                           CEVLAN: 1
VPN name     :                               Is Router: TRUE
------------------------------------------------------------------------------
Total: 1       Dynamic: 0       Static: 1
```

**Table 6-63** 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 the neighbor. |

| Item | Description |
| --- | --- |
| State | Status of a neighbor entry:<br>• 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.<br>• 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.<br>• 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.<br>• 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.<br>• 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:<br>• The aging time of static entries is displayed as "-".<br>• The aging time of dynamic entries is the time that the reachable state lasts. "#" indicates non-reachable (only for dynamic entries). |
| VLAN | ID of the VLAN to which the neighbor belongs. |
| CEVLAN | ID of the CEVLAN to which a neighbor belongs.<br>**NOTE**<br>Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this parameter. |
| VPN name | Name of a VPN instance to which the neighbor belongs. |

| Item | Description |
| --- | --- |
| Is Router | Whether an NA packet carries the R flag:<br>• If the NA packet carries the R flag, "TRUE" is displayed.<br>In this case, the neighbor is a routing device.<br>• If the NA packet carries no R flag, "FALSE" is displayed.<br>In this case, the neighbor may be a PC or a routing device that sends an NA packet carrying no R flag. |
| Total | Number of total neighbor entries. |
| Dynamic | Number of dynamic neighbor entries. |
| Static | Number of static neighbor entries. |

# 6.10.9 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 |
| --- | --- | --- |
| *ipv6-address* | Displays PMTU entries that match 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. | - |
| **vpn-instance** *vpn-instance-name* | Displays PMTU entries of a specified IPv6 VPN instance. | The value must be an existing VPN instance name. |

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

### Usage Scenario

If the MTU on the outbound interface of an intermediate routing device is smaller than the MTU of the source host, 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 **ipv6 pathmtu** command, no static PMTU entry is displayed after the **display ipv6 pathmtu** command is run.

If a static PMTU entry is displayed, the remaining lifetime displays "-".

## Example

# Display all PMTU entries.

```
<HUAWEI> display ipv6 pathmtu all
IPv6 Destination Address              ZoneID PathMTU LifeTime(M) Type    FF
FC00::2                                    0    1500    -          Static  NO
-------------------------------------------------------------------------------
Total: 1      Dynamic: 0     Static: 1
```

**Table 6-64** Description of the display ipv6 pathmtu command output

| Item | Description |
| --- | --- |
| IPv6 Destination Address | Destination IPv6 address. |
| ZoneID | Zone ID. |
| PathMTU | PMTU of an IPv6 address.<br>To configure the PMTU for an IPv6 address, run the **ipv6 pathmtu** command. |
| LifeTime(M) | Remaining lifetime, in minutes. The update interval is 1 minute. This field displays "-" for static entries. |

| Item | Description |
| --- | --- |
| Type | Type of the PMTU entry:<br>• Dynamic: dynamic entries<br>• Static: static entries (configured through CLI) |
| FF | Fragmentation flag:<br>• YES: Packets are fragmented, and a fragment header is added to a packet.<br>• NO: Packets are not fragmented. |
| Total | Total number of PMTU entries. |
| Dynamic | Number of dynamic PMTU entries. |
| Static | Number of static PMTU entries. |

# 6.10.10 display ipv6 socket

## Function

The **display ipv6 socket** command displays information about IPv6 sockets.

## Format

**display ipv6 socket** [ **socktype** *socket-type* | **task-id** *task-id* **socket-id** *socket-id* ]

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **socktype** *socket-type* | Specifies the type of a socket. The value can be:<br>• 1: indicates SOCK_STREAM, corresponding to the TCP-based socket.<br>• 2: indicates SOCK_DGRAM, corresponding to the UDP-based socket.<br>• 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. |

| Parameter | Description | Value |
| --- | --- | --- |
| **task-id** *task-id* | Specifies the task ID. | The value is an integer and the range depends on the task configuration. |

## 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.

If no parameter is specified, this command displays information about all types of sockets.

## Example

# Display information about all types of sockets.

```
<HUAWEI> display ipv6 socket
SOCK_STREAM:
Task = VTYD(102), socketid = 3, Proto = 6,
LA = ::->22, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEADDR SO_KEEPALIVE SO_LINGER SO_SETACL6 SO_
SETKEEPALIVE SO_ZONEID(-1),
socket state = SS_PRIV SS_ASYNC

Task = VTYD(102), socketid = 2, Proto = 6,
LA = ::->23, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_KEEPALIVE SO_LINGER SO_REUSEPORT SO_SETACL6 SO_
SETKEEPALIVE SO_ZONEID(-1),
socket state = SS_PRIV SS_ASYNC

SOCK_DGRAM:
Task = TRAP(105), socketid = 2, Proto = 17,
LA = ::->49152, FA = ::->0,
sndbuf = 9216, rcvbuf = 42080, sb_cc = 0, rb_cc = 0,
socket option = SO_ZONEID(-1),
socket state = SS_PRIV

Task = AGT6(106), socketid = 1, Proto = 17,
LA = ::->161, FA = ::->0,
sndbuf = 17941, rcvbuf = 42080, sb_cc = 0, rb_cc = 0,
socket option = SO_ZONEID(-1),
socket state = SS_PRIV SS_ASYNC
```

```
Task = RDS(123), socketid = 2, Proto = 17,
LA = ::->1812, FA = ::->0,
sndbuf = 9216, rcvbuf = 42080, sb_cc = 0, rb_cc = 0,
socket option = SO_ZONEID(-1),
socket state = SS_PRIV SS_RECALL

SOCK_DGRAM:
SOCK_RAW:
```

# Display information about the socket with socket type 1.

```
<HUAWEI> display ipv6 socket socktype 1
SOCK_STREAM:
Task = VTYD(102), socketid = 3, Proto = 6,
LA = ::->22, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEADDR SO_KEEPALIVE SO_LINGER SO_SETACL6 SO_
SETKEEPALIVE SO_ZONEID(-1),
socket state = SS_PRIV SS_ASYNC

Task = VTYD(102), socketid = 2, Proto = 6,
LA = ::->23, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_KEEPALIVE SO_LINGER SO_REUSEPORT SO_SETACL6 SO_
SETKEEPALIVE SO_ZONEID(-1),
socket state = SS_PRIV SS_ASYNC
```

**Table 6-65** Description of the **display ipv6 socket** command output

| Item | Description |
| --- | --- |
| SOCK_STREAM | One type of socket. Sockets are classified into the following types:<br>• SOCK_STREAM<br>• SOCK_DGRAM<br>• SOCK_RAW |
| Task = VTYD | Type and ID of the task that invokes the socket. For example, **Task = VTYD(48)** shows that the task named VTYD uses the socket, with task ID 48. |
| socketid | Socket ID. |
| Proto | Protocol ID. |
| LA | Local address and local port number. |
| FA | Remote address and remote port number. |
| sndbuf | Upper limit of the send buffer, in bytes. |
| rcvbuf | Upper limit of the receive buffer, in bytes. |
| sb_cc | Total number of sent bytes. |
| rb_cc | Total number of received bytes. |
| socket option | Socket option that has been set. |
| socket state | Socket status. |

# 6.10.11 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.<br>• *interface-type* specifies the interface type.<br>• *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:
   Total             : 0
   Local sent out    : 0          Forwarded         : 0
   Raw packets       : 0          Discarded         : 0
   Fragmented        : 0          Fragments         : 0
   Fragments failed  : 0          Multicast         : 0

 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 6-66** 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. |

| 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. |
| Reassembly 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 number of the IPv6 extension headers. |
| Hop-by-Hop Options | Total number of the hop-by-hop options headers. |
| Mobility Header | Total number of the mobility headers. |
| Destination Options | Total number of the destination options headers. |

| Item | Description |
| --- | --- |
| Routing Header | Total number of the routing options headers. |
| Fragment Header | Total number of the fragment headers. |
| Authentication Header | Total number of the authentication headers. |
| Encapsulation Header | Total number of the encapsulation headers. |
| No header | Total number of the packets without headers. |
| TLV Length error | Total number of the extension headers in which the TLV length field is wrong. |
| Header Length error | Total number of the extension headers in which the length field is wrong. |
| Unknown header type | Total number of the unknown extension header types. |
| Unknown TLV type | Total number of the unknown TLV types. |

# 6.10.12 display nd optimized-passby status

## Function

The **display nd optimized-passby status** command displays whether the device is configured not to send NS packets destined for other devices to the CPU and whether the configuration takes effect.

## Format

**display nd optimized-passby status interface vlanif** *vlanif-id* **slot** *slot-id*

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **interface vlanif** *vlanif-id* | Displays whether the device is configured not to send NS packets destined for other devices to the CPU and whether the configuration takes effect on a specified VLANIF interface. | The value is an integer and the value range depends on the range of existing VLANIF interfaces. You can enter ? to obtain the range of VLANIF interface numbers. |
| **slot** *slot-id* | Displays whether the device is configured not to send NS packets destined for other devices to the CPU and whether the configuration takes effect in a specified slot. | The value must be set according to the device configuration. |

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

If an interface receives a large number of NS packets whose destination IPv6 addresses are different from the IPv6 address of this interface and sends these NS packets to the CPU for processing, the CPU usage is high and the CPU cannot process services properly.

To prevent this issue, you can configure the device to directly forward NS packets destined for other devices without sending them to the CPU. This improves the device's capability of defending against packet attacks.

When the device is configured not to send NS packets destined for other devices to the CPU, the configuration does not take effect if a conflict configuration exists on the device. You can use the **display nd optimized-passby status** command to check whether the device is configured not to send NS packets destined for other devices to the CPU and whether the configuration takes effect. For details about conflict configurations, see **nd optimized-passby enable**.

## Example

# Display whether the device is configured not to send NS packets destined for other devices to the CPU and whether the configuration takes effect on VLANIF 100.

```
<HUAWEI> display nd optimized-passby status interface Vlanif 100 slot 0
Current configuration: Enable
Actual        status: Inactive
Inactive      Reason: The interface protocol status is down.
```

**Table 6-67** Description of the **display nd optimized-passby status** command output

| Item | Description |
| --- | --- |
| Current configuration | Whether the device is configured not to send NS packets destined for other devices to the CPU.<br>• Enable: The device is configured not to send NS packets destined for other devices to the CPU.<br>• Disable: The device is configured to send NS packets destined for other devices to the CPU. |
| Actual status | Whether the configuration of disabling the device from sending NS packets destined for other devices to the CPU takes effect.<br>• Inactive<br>• Active |
| Inactive Reason | Conflict configuration. |

# 6.10.13 display nd optimized-reply statistics

## Function

The **display nd optimized-reply statistics** command displays statistics on optimized ND Reply packets.

## Format

**display nd optimized-reply statistics** [ **slot** *slot-id* ]

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **slot** *slot-id* | Specifies the stack ID. | The value is an integer. It has a fixed value of 0 in a non-stack scenario, and depends on the device configuration in a stack scenario. |

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

You can run this command to check statistics on optimized ND Reply packets after the optimized ND reply function is enabled on the device.

## Example

# Display statistics on optimized ND Reply packets.

```
<HUAWEI> display nd optimized-reply statistics
Slot          Received          Processed          Dropped
------------------------------------------------------------------
0             11                9                  7
```

**Table 6-68** Description of the display nd optimized-reply statistics command output

| Item | Description |
| --- | --- |
| Slot | Stack ID. |
| Received | Number of ND Request packets entering the processing procedure of the optimized ND reply function. |
| Processed | Number of optimized ND Reply packets. |
| Dropped | Number of ND Request packets discarded.<br>**NOTE**<br>When the optimized ND reply function is enabled, the device does not optimize the responses to the ND Request packets whose destination IPv6 address is not the IPv6 address of a local interface on the switch. |

# 6.10.14 display nd optimized-reply status

## Function

The **display nd optimized-reply status** command displays the status of the optimized ND reply function.

## Format

**display nd optimized-reply status**

## Parameters

None

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

You can run this command to check the status of the optimized ND reply function.

## Example

# Check the status of the optimized ND reply function.

```
<HUAWEI> display nd optimized-reply status
Current configuration:Disable
Actual         status:Inactive
Related configuration:
  nd optimized-reply disable
```

**Table 6-69** Description of the display nd optimized-reply status command output

| Item | Description |
| --- | --- |
| Current configuration | Configuration of the optimized ND reply function.<br>• Enable<br>• Disable<br>To set this field, run the **nd optimized-reply disable** command. |
| Actual status | Status of the optimized ND reply function.<br>• Active<br>• Inactive |
| Related configuration | Configuration that results in the invalid optimized ND reply function.<br>If the optimized ND reply function has taken effect, this field is not displayed. |

# 6.10.15 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

## 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 6-70** 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. |

| Item | Description |
| --- | --- |
| 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. |

# 6.10.16 display tcp ipv6 authentication-statistics

## Function

The **display tcp ipv6 authentication-statistics** command displays authentication statistics of a specified TCP6 connection.

## 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 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. |
| **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 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. |
| **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
    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 6-71** Description of the **display tcp ipv6 authentication-statistics** command output

| Item | Description |
| --- | --- |
| total (received packets) | Total number of received and discarded TCP6 packets. |
| 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. |

| Item | Description |
| --- | --- |
| 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. |
| total (sent packets) | Total number of sent and unsent TCP6 packets. |
| 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. |

# 6.10.17 display tcp ipv6 statistics

## Function

The **display tcp ipv6 statistics** command displays TCP6 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, for example:

- Established connections: indicates the number of established connections, helping you determine whether to continue deploying services such as BGP services or adjust the load.
- Duplicate ACK packets: indicates 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: allows you 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 TCP6 statistics within a specified period, run the **reset tcp ipv6 statistics** command to clear existing statistics.

## Example

# Display TCP6 packet statistics.

```
<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

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

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: 1 (dropped: 0, initiated dropped: 0)
```

**Table 6-72** Description of the **display tcp ipv6 statistics** command output

| Item | Description |
| --- | --- |
| Received packets:<br>total | Total number of received packets. |
| packets in sequence | Number of packets received in sequence. |
| window probe packets | Number of received window probe packets. |
| window update packets | Number of received window update packets. |
| checksum error | Number of received packets received 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. |
| Sent packets:<br>total | 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. |

| Item | Description |
| --- | --- |
| 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. |
| 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. |

# 6.10.18 display tcp ipv6 status

## Function

The **display tcp ipv6 status** command displays the status of all TCP6 connections.

## Format

**display tcp ipv6 status** [ **local-ip** *ipv6-address* ] [ **local-port** *local-port-number* ] [ **remote-ip** *ipv6-address* ] [ **remote-port** *remote-port-number* ]

**display tcp ipv6 status** [ **task-id** *task-id* [ **sock-id** *sock-id* ] ]

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **local-ip** *ipv6-address* | Displays the TCP6 connection status of the specified IPv6 address. *ipv6-address* specifies the 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. |
| **remote-ip** *ipv6-address* | Displays the TCP6 connection status of the specified IPv6 address. *ipv6-address* specifies the IPv6 address of the remote 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. |
| **local-port** *local-port-number* | Displays the TCP6 connection status of the specified port number. *local-port-number* specifies the port number of the local device. | The value is an integer that ranges from 0 to 65535. |
| **remote-port** *remote-port-number* | Displays the TCP6 connection status of the specified port number. *remote-port-number* 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 TCP6 connection with the specified task ID. *task-id* specifies the task ID. | The value is an integer that ranges from 1 to 200. |
| **sock-id** *sock-id* | Displays the TCP6 connection status with the specified socket ID. *sock-id* specifies the 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 TCP6 control blocks, including the following information:

- TCP6 socket ID
- Local IPv6 address and port number
- Remote IPv6 address and port number
- TCP6 connection status
- VPN ID

To view the status of all valid TCP6 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 TCP6 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 TCP6 connections.

```
<HUAWEI> display tcp ipv6 status
* - MD5 Authentication is enabled.
TCP6CB   TID/SoID  Local Address       Foreign Address      State       VPNID
0be58fa8 102/3     ::->22              ::->0                Listening   0
0d109448 102/2     ::->23              ::->0                Listening   0
```

**Table 6-73** Description of the **display tcp ipv6 status** command output

| Item | Description |
| --- | --- |
| TCP6CB | Address of a TCP6 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. |

| Item | Description |
| --- | --- |
| State | Status of a TCP6 connection:<br>• Closed: indicates that the TCP connection is closed.<br>• Listening: indicates that the TCP connection is being listened on.<br>• Syn_Rcvd: indicates that a TCP packet with the SYN flag is received.<br>• Syn_Sent: indicates that a TCP packet with the SYN flag is sent.<br>• Established: indicates that the TCP connection has been set up.<br>• 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.<br>• 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.<br>• 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.<br>• 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.<br>• Closing: indicates that the two ends close the TCP connection simultaneously.<br>• LAST_ACK: indicates that the local end waits for acknowledging the TCP connection teardown request sent to the remote end. |
| VPNID | VPN ID. |

# 6.10.19 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

1: Monitoring 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 VLANIF10.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] display this ipv6 interface
Vlanif10 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::2E0:4AFF:FE3D:9801 [TENTATIVE]
  Global unicast address(es):
    FC00::1, subnet is FC00::/64 [TENTATIVE]
  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
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisement max interval 600 seconds, min interval 200 seconds
  ND router advertisements live for 1800 seconds
  ND router advertisements hop-limit 64
  ND default router preference medium
  Hosts use stateless autoconfig for addresses
```

# Display IPv6 information on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 address fc00:1::1 64
[HUAWEI-GigabitEthernet0/0/1] display this ipv6 interface
GigabitEthernet0/0/1 current state : DOWN
IPv6 protocol current state : DOWN
IPv6 is enabled, link-local address is FE80::225:9EFF:FEF4:ABCD
[TENTATIVE]
  Global unicast address(es):
    FC00:1::1, subnet is FC00:1::/64 [TENTATIVE]
  Joined group address(es):
    FF02::1:FF00:1
    FF02::1:FFF4:ABCD
    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
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisement max interval 600 seconds, min interval 200 seconds
  ND router advertisements live for 1800 seconds
  ND router advertisements hop-limit 64
  ND default router preference medium
  Hosts use stateless autoconfig for addresses
```

**Table 6-74** Description of the **display this ipv6 interface** command output

| Item | Description |
| --- | --- |
| Vlanif10 current state | Current physical status of VLANIF 10.<br>● UP: enabled<br>● DOWN: disabled |
| GigabitEthernet0/0/1 current state | Current physical status of GigabitEthernet0/0/1.<br>● UP: enabled<br>● DOWN: disabled |
| IPv6 protocol current state | Current protocol status of the interface.<br>● UP: enabled<br>● DOWN: disabled |
| link-local address | Link-local address on the interface.<br>After an IPv6 address is configured on the interface, the system automatically assigns a link-local address for the interface. To manually configure a link-local address for an interface, run the **ipv6 address link-local** command. |

| Item | Description |
| --- | --- |
| Global unicast address(es) | Global unicast address configured on the interface.<br>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. |
| TENTATIVE | When the interface is in DOWN state, the IPv6 address is TENTATIVE.<br>When the IPv6 address is duplicate with another, this field is DUPLICATE.<br>In normal cases, this field is not displayed. |
| MTU | MTU of the interface.<br>To configure the MTU for an interface, run the **ipv6 mtu** command. |
| ND DAD is enabled | Duplicate address detection (DAD) has been enabled. |
| number of DAD attempts | Number of times duplicate address detection is performed. |
| ND reachable time | Neighbor reachable time. |
| ND retransmit interval | Retransmission interval. |
| ND stale time | Aging time of ND entries in STALE state. |
| ND advertised reachable time | Reachable time of NA packets.<br>**NOTE**<br>This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface. |
| ND advertised retransmit interval | Retransmission interval of NA packets.<br>**NOTE**<br>This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface. |
| ND router advertisement max interval 600 seconds, min interval 200 seconds | Maximum and minimum interval of RA packets.<br>**NOTE**<br>This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface. |
| ND router advertisements live for | Router lifetime in RA packets.<br>**NOTE**<br>This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface. |

| Item | Description |
| --- | --- |
| ND router advertisements hop-limit | Hop limit of RA packets.<br>**NOTE**<br>This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface. |
| ND default router preference | Default route priority in RA packets.<br>**NOTE**<br>This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface. |
| Hosts use stateless autoconfig for addresses | Hosts obtain IPv6 addresses by means of stateless auto-configuration.<br>**NOTE**<br>This field is displayed only after the **undo ipv6 nd ra halt** command is executed on the interface. |

# 6.10.20 display udp ipv6 statistics

## Function

The **display udp ipv6 statistics** command displays UDP6 packet statistics.

## Format

**display udp ipv6 statistics**

## Parameters

None

## Views

All views

## Default Level

1: Monitoring level

## 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 UDP6 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 UDP6 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: 1

Sent packets:
    total: 0
    total(64bit high-capacity counter): 0
```

**Table 6-75** 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 UDP6 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. |
| 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. |

# 6.10.21 eth-trunk (tunnel interface view)

## Function

The **eth-trunk** command associates a specified tunnel interface with an Eth-Trunk interface enabled with service loopback.

The **undo eth-trunk** command disassociates a specified tunnel interface from an Eth-Trunk interface enabled with service loopback.

NOTE

Only the S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

## Format

**eth-trunk** *trunk-id*

**undo eth-trunk**

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *trunk-id* | Specifies the ID of an Eth-Trunk interface associated with the tunnel interface. | S5720I-SI, S5735-S, S500, S5735-S-I, and S5735S-S: The value ranges from 0 to 119.<br>S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S: The value ranges from 0 to 127.<br>S5735S-H, S5736-S, and S6720S-S: The value ranges from 0 to 249. |

## Views

Tunnel interface view

## Default Level

2: Configuration level

## Usage Guidelines

Before associating a specified tunnel interface with an Eth-Trunk interface, run the **service type tunnel** command to enable service loopback on the Eth-Trunk interface.

## Example

# Associate Tunnel1 with the Eth-Trunk interface enabled with service loopback.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] eth-trunk 1
```

# 6.10.22 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.

NOTE

The **undo ipv6** command disables the device from forwarding IPv6 unicast packets. Therefore, confirm your action before running this command.

When system resources are insufficient, the **ipv6** command does not take effect and an alarm is generated. The alarm ID is 1.3.6.1.4.1.2011.5.25.227.2.1.7.

## Example

# Enable the device to forward IPv6 unicast packets.

```
<HUAWEI> system-view
[HUAWEI] ipv6
```

# Disable the device from forwarding IPv6 unicast packets.

```
<HUAWEI> system-view
[HUAWEI] undo ipv6
Warning: This operation will interrupt all IPv6 services. Continue?[Y/N]:y
```

# 6.10.23 ipv6 address

## Function

The **ipv6 address** command configures a site-local address or 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. |

| Parameter | Description | Value |
| --- | --- | --- |
| *prefix-length* | Specifies the prefix length of an IPv6 address.<br>An IPv6 address with a 128-bit prefix can be configured only on a loopback interface. | The value is an integer that ranges from 1 to 128. |
| *dhcpv6-prefix* | Specifies the prefix assigned to a DHCPv6 PD client. | The value must be an existing prefix assigned to a DHCPv6 PD client. |

## 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 switch 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 switch uses the prefix assigned to the DHCPv6 PD client and the IPv6 address to form an RA prefix for the interface only when the switch 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 switch:

- 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 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.

The following IPv6 addresses cannot be configured for an interface:

- Loopback address (::1/128)
- Unspecified address (::/128)
- Multicast address
- IPv4-mapped IPv6 address (0:0:0:0:0:FFFF:IPv4-address)

A 128-bit IPv6 address has two formats:

- X:X:X:X:X:X:X:X

  In this format, a 128-bit IPv6 address is written as eight groups of four hexadecimal digits (0 to 9, A to F), where each group is separated by a colon (:). Every X represents a group of hexadecimal numbers.
- X:X:X:X:X:X:d.d.d.d

  In this format, "X:X:X:X:X:X" represent the high-order six groups of numbers, and each X stands for 16 bits that are represented by four hexadecimal characters. "d.d.d.d" represents the low-order four groups of numbers, and each d stands for 8 bits that are represented by decimal numbers. "d.d.d.d" stands for a standard IPv4 address.

An IPv6 address has two parts:

- Network prefix: corresponds to the network ID of an IPv4 address. It is of n bits.
- Interface identifier: corresponds to the host ID of an IPv4 address. It is of 128-n bits.

If the **ipv6 address** command has been run to configure an IPv6 address for an interface, but no link-local address is configured for the interface, the system generates a link-local address for the interface.

If no parameter (IPv6 address or prefix length) is specified in the **undo ipv6 address** command, running the **undo ipv6 address** command deletes all IPv6 addresses.

## Example

# Configure a global unicast address for VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 address fc00::1/64
```

# Configure a global unicast address for GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
```

```
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 address fc00::1/64
```

# Configure an IPv6 address bound to the DHCPv6 PD prefix for VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 address prefix1 ::1:0:0:0:1/64
```

# 6.10.24 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. |

## 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. If an anycast address is used, you need to configure the same address for the tunnel interfaces of all devices. In this manner, the number of addresses is reduced.

**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 2002:c058:6301::/48 for VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 address 2002:c058:6301:: 48 anycast
```

# Configure anycast address 2002:c058:6301::/48 for GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 address 2002:c058:6301:: 48 anycast
```

# 6.10.25 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** [ **default** ]

**undo ipv6 address auto global**

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **default** | Indicates that the device learns the default route. | - |

## 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 configure a link-local address to interconnect with local nodes.

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 VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 address auto global
```

# Enable a device to generate an IPv6 global address through stateless autoconfiguration on interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 address auto global
```

# 6.10.26 ipv6 address auto link-local

## Function

The **ipv6 address auto link-local** command configures an interface to automatically generate a link-local address.

The **undo ipv6 address auto link-local** command deletes the automatically generated link-local address on a specified interface.

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

Link-local addresses are used for communications between link-local nodes in either the neighbor discovery or stateless auto-configuration process. A packet

with a link-local address set to a source or destination address will not be forwarded to another link. That is, link-local addresses are valid only on local links.

After the **ipv6 address auto link-local** command is run, a device uses the link-local address prefix FE80::/10 (1111 1110 10) and IEEE EUI-64 interface identifier go generate a link-local address for an interface. An IEEE EUI-64 interface identifier is converted from an interface link layer address, for example a MAC address.

1. The hexadecimal number FFFE (1111 1111 1111 1110 in binary) is inserted in the middle of a MAC address.
2. The U/L bit (the leftmost seventh bit) is set to 1.
3. The interface ID in EUI-64 format then is obtained.

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.

**Precautions**

Only a single link-local address can be assigned to each interface. If an automatically allocated link-local address has already been configured on an interface, running the **ipv6 address link-local** command will overwrite the existing link-local address.

The **undo ipv6 address auto link-local** command can only delete a link-local address that is automatically generated by an interface. To delete a manually configured link-local address, run the **undo ipv6 address link-local** command.

## Example

# Configure VLANIF2 to automatically generate a link-local address.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 2
[HUAWEI-Vlanif2] ipv6 enable
[HUAWEI-Vlanif2] ipv6 address auto link-local
```

# Configure GE0/0/1 to automatically generate a link-local address.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 address auto link-local
```

# 6.10.27 ipv6 address eui-64

## Function

The **ipv6 address eui-64** command configures a site-local address or global unicast address in EUI-64 format for an interface.

The **undo ipv6 address eui-64** command deletes a site-local address or global unicast address in EUI-64 format from an interface.

By default, no site-local address or 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. |

## 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.

**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 switch:

- 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 maximum of 10 global unicast addresses can be configured for an interface.

The following IPv6 addresses in EUI-64 format cannot be configured for an interface:

- Loopback address (::1/128)
- Unspecified address (::/128)
- Multicast address
- IPv4-mapped IPv6 address (0:0:0:0:0:FFFF:IPv4-address)

The **ipv6 address** command is used to specify a 128–bit IPv6 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 IPv6 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 an IPv6 address in EUI-64 format for VLANIF 2.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 2
[HUAWEI-Vlanif2] ipv6 enable
[HUAWEI-Vlanif2] ipv6 address fc00::1/64 eui-64
```

# Configure an IPv6 address in EUI-64 format for GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 address fc00::1/64 eui-64
```

# 6.10.28 ipv6 address link-local

## Function

The **ipv6 address link-local** command manually configures a link-local address for a specified interface.

The **undo ipv6 address link-local** command deletes the manually configured link-local address on an interface.

By default, no link-local address is configured for an interface.

## 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. The packet with a link-local address being the source or destination address will not be forwarded to other links. That is, link-local addresses are valid only on local links.

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 **undo ipv6 address link-local** command deletes only the link-local address manually configured for an interface. To delete the automatically generated link-local address, run the **undo ipv6 address auto link-local** command.

If an 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.

The following IPv6 addresses cannot be configured for an interface:

- Loopback address (::1/128)
- Unspecified address (::/128)
- Multicast address

## Example

# Manually configure a link-local address for VLANIF 2.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 2
[HUAWEI-Vlanif2] ipv6 enable
[HUAWEI-Vlanif2] ipv6 address fe80::1 link-local
```

# Manually configure a link-local address for GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 address fe80::1 link-local
```

# 6.10.29 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.

**Follow-up Procedure**

Configure IPv6 addresses and ND parameters. ND parameters include the M flag, O flag, RA halt flag, interval for sending RA packets, lifetime of RA packets, interval for sending NS packets, DAD counts, period during which the IPv6 neighbor keeps reachable, prefix carried in the RA packet, and static ND entries.

**Precautions**

After the IPv6 function is disabled on an interface, IPv6 configurations on the interface are deleted.

- After the IPv6 function is disabled on an interface, IPv6 addresses of the interface are deleted and IPv6 commands cannot be configured on the interface.
- After the IPv6 function is disabled on an interface, IS-IS IPv6 and RIPng are disabled on the interface. That is, the **isis ipv6 enable** and **ripng enable** commands become ineffective.

When system resources are insufficient, the **ipv6 enable** command does not take effect and an alarm is generated. The alarm ID is 1.3.6.1.4.1.2011.5.25.227.2.1.22.

## Example

# Enable the IPv6 function on VLANIF10.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ipv6 enable
```

# Enable the IPv6 function on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
```

# 6.10.30 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

## 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.

The token bucket algorithm is used to count ICMPv6 packets. One token represents an ICMPv6 error 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. Once the number of ICMPv6 packets exceeds the maximum number of tokens that the bucket can contain, excess 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
```

# 6.10.31 ipv6 icmp blackhole unreachable send

## Function

The **ipv6 icmp blackhole unreachable send** command enables the switch 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 switch from sending a Destination Unreachable ICMP packet to an initiator when a tracert packet matches an IPv6 blackhole route.

By default, the switch 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 switch configured with the user access and authentication function, when a user goes offline, only the IPv6 blackhole route corresponding to the user's address segment exists on the switch. When a tracert packet matches the IPv6 blackhole route, the switch discards the packet. As a result, an initiator cannot detect that the user has gone offline.

After you run the **ipv6 icmp blackhole unreachable send** command, the switch 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 switch.

## Example

# Enable the switch 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
```

# 6.10.32 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.

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 VLANIF100 to send ICMPv6 Port Unreachable messages.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 icmp port-unreachable send
```

# Enable interface GE0/0/1 to send ICMPv6 Port Unreachable messages.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 icmp port-unreachable send
```

# 6.10.33 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.

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 VLANIF100 from sending ICMPv6 Hop Limit Exceeded messages.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] undo ipv6 icmp hop-limit-exceeded send
```

# Disable interface GE0/0/1 from sending ICMPv6 Hop Limit Exceeded messages.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] undo ipv6 icmp hop-limit-exceeded send
```

# 6.10.34 ipv6 icmp receive

## Function

The **ipv6 icmp receive** command enables the system to receive ICMPv6 messages with the local address as the destination address.

The **undo ipv6 icmp receive** command disables the system from receiving ICMPv6 messages with the local address as the destination address.

By default, the system receives ICMPv6 messages with the local address as the destination address.

## 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 messages. | The value is an integer in the range from 0 to 255. |
| *icmpv6-code* | Specifies the code of ICMPv6 messages. | The value is an integer in the range from 0 to 255. |
| *icmpv6-name* | Specifies the name of ICMPv6 messages. | ICMPv6 messages are classified into the following types:<br>● echo: Echo packet<br>● echo-reply: Echo Reply packet<br>● err-header-field: Packet with an error header<br>● frag-time-exceeded: Fragmentation Timeout packet<br>● hop-limit-exceeded: Packet whose hop count exceeds the limit<br>● host-admin-prohib: Packet that is rejected by a host<br>● host-unreachable: ICMPv6 Host Unreachable packet<br>● neighbor-advertisement: Neighbor Advertisement packet<br>● neighbor-solicitation: Neighbor Solicitation packet<br>● network-unreachable: ICMPv6 Network Unreachable packet<br>● packet-too-big: Packet Too Big packet<br>● port-unreachable: ICMPv6 Port Unreachable packet<br>● redirect: Redirected packets<br>● router-advertisement: Router Advertisement packet<br>● router-solicitation: Router Solicitation packet<br>● unknown-ipv6-opt: Error packet with unknown options<br>● unknown-next-hdr: Error packet with unknown next header |
| **all** | Indicates all ICMPv6 messages. | - |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

In normal cases, a switch can properly receive ICMPv6 messages. However, when network traffic load is heavy, host unreachable or port unreachable events frequently occur, the switch receives a large number of ICMPv6 messages, which burdens the network and degrades device performance. In addition, attackers usually use ICMPv6 error messages 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 with the local address as the destination address.

**Precautions**

When the network is in good performance again, you can run the **ipv6 icmp receive** command to enable the system to receive ICMPv6 messages with the local address as the destination address.

After the **undo ipv6 icmp receive** command is run, main interfaces are disabled from processing these ICMPv6 messages. In addition, the system does not collect statistics on these messages that are received but collects statistics on discarded messages.

## Example

# Disable the system from receiving ICMPv6 Echo packets with the local address as the destination address.

```
<HUAWEI> system-view
[HUAWEI] undo ipv6 icmp echo receive
```

# 6.10.35 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.

## 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:<br>• echo: Echo packet<br>• echo-reply: Echo Reply packet<br>• err-header-field: Packet with an error header<br>• frag-time-exceeded: Fragmentation Timeout packet<br>• hop-limit-exceeded: Packet whose hop count exceeds the limit<br>• host-admin-prohib: Packet that is rejected by a host<br>• host-unreachable: ICMPv6 Host Unreachable packet<br>• neighbor-advertisement: Neighbor Advertisement packet<br>• neighbor-solicitation: Neighbor Solicitation packet<br>• network-unreachable: ICMPv6 Network Unreachable packet<br>• packet-too-big: Packet Too Big packet<br>• port-unreachable: ICMPv6 Port Unreachable packet<br>• redirect: Redirected packets<br>• router-advertisement: Router Advertisement packet<br>• router-solicitation: Router Solicitation packet<br>• unknown-ipv6-opt: Error packet with unknown options<br>• unknown-next-hdr: Error packet with unknown next header |

| 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.

```
<HUAWEI> system-view
[HUAWEI] undo ipv6 icmp all send
```

# 6.10.36 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**

## 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
```

# 6.10.37 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 S5732-H, S6730-S, S6730S-S, S6730S-H, and S6730-H, this command does not take effect on the IPv6 packets matching ND entries. That is, the MTU of IPv6 packets matching ND entries on the devices is always 1500 bytes.

## Format

**ipv6 mtu** *mtu*

**undo ipv6 mtu**

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *mtu* | Specifies the MTU value. | • For GE interfaces, GE sub-interfaces, XGE interfaces, XGE sub-interfaces, MultiGE interfaces, MultiGE sub-interfaces, 25GE interfaces, 25GE sub-interfaces, tunnel interfaces, and VLANIF interfaces, the value is an integer that ranges from 1280 to 9600, in bytes.<br>• For other interfaces, the value is an integer that ranges from 1280 to 1500, in bytes.<br>The default value is 1500. |

## Views

Interface view

## Default Level

2: Configuration level

## Usage Guidelines

### Usage Scenario

If the traffic processing capability of a link connecting the source and destination ends changes, you can use this command to set the MTU of IPv6 packets on an interface. If the packet length is larger than the IPv6 MTU of the interface, the system fragments the packet based on the configured MTU value before forwarding the packet.

### Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

### Precautions

The directly-connected interfaces must be configured with the same IPv6 MTU values.

## Example

# Set the MTU of IPv6 packets on VLANIF2 to 1280 bytes.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 2
[HUAWEI-Vlanif2] ipv6 enable
[HUAWEI-Vlanif2] ipv6 mtu 1280
```

# Set the MTU of IPv6 packets on GE0/0/1 to 1280 bytes.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 mtu 1280
```

# 6.10.38 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.

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**

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.

## Example

# Set the M flag of stateful autoconfiguration in an RA packet on VLANIF2.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 2
[HUAWEI-Vlanif2] ipv6 enable
[HUAWEI-Vlanif2] ipv6 nd autoconfig managed-address-flag
```

# Set the M flag of stateful autoconfiguration in an RA packet on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd autoconfig managed-address-flag
```

# 6.10.39 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.

**Prerequisites**

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

## Example

# Set the O flag of stateful autoconfiguration on VLANIF2.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 2
[HUAWEI-Vlanif2] ipv6 enable
[HUAWEI-Vlanif2] ipv6 nd autoconfig other-flag
```

# Set the O flag of stateful autoconfiguration on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd autoconfig other-flag
```

# 6.10.40 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**

## 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. The default number of detection times is recommended. If there is a long link delay, you can increase the number of detection times. When a loopback address is configured for an interface, the loopback address may fail the address conflict detection. In this case, you can set the number of detection times to 0 to disable detection, allowing the loopback address to be used.

**Prerequisites**

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

**Precautions**

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.

If the **ipv6 nd dad attempts** command has been run, running the **ipv6 nd ra** command will change the number of configured detection times.

DAD transmits node configuration variables. The system automatically determines the time to send neighbor request messages while DAD is performed to detect a tentative unicast IPv6 address.

## Example

# Set the number of times NS packets are sent when the system performs DAD to 20 on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
```

```
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 nd dad attempts 20
```

# Set the number of times NS packets are sent when the system performs DAD to 20 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd dad attempts 20
```

# 6.10.41 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 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.

- 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.

```
<HUAWEI> system-view
[HUAWEI] ipv6 nd hop-limit 100
```

# 6.10.42 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**

## 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, VBDIF interface view, Eth-Trunk interface view, Eth-Trunk sub-interface view, system view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

Generally, a device uses neighbor advertisement (NA) packets to establish neighbor entries. 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.

**Prerequisites**

Before using the **ipv6 nd learning strict** command to enable IPv6 neighbor discovery (ND) strict learning on an interface, ensure that the IPv6 function has been enabled on the interface using the **ipv6 enable** command.

**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. For the models supporting switching between Layer 2 and Layer 3 modes, see **portswitch**.

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
```

# 6.10.43 ipv6 nd link-local-entry-learn enable

## Function

The **ipv6 nd link-local-entry-learn enable** command enables the device to learn the ND entry containing the link-local address of a peer interface.

The **undo ipv6 nd link-local-entry-learn enable** command disables the device from learning the ND entry containing the link-local address of a peer interface.

By default, the device is disabled from learning the ND entry containing the link-local address of a peer interface.

## Format

**ipv6 nd link-local-entry-learn enable**

**undo ipv6 nd link-local-entry-learn enable**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

By default, on a network where IPv6 routes are learnt through RIPng, a device can learn the link-local address of a peer interface only through packets. If a device does not learn the link-local address of a peer interface but needs to forward a packet with the next hop being this address, the packet will be lost.

The **ipv6 nd link-local-entry-learn enable** command helps solve this issue. With this command run on a device on a RIPng network, the device learns the ND entry containing the link-local address of a peer interface, when it learns the ND entry containing the global unicast address of the peer interface. If you do not require this function, you are advised to disable this function to reduce the memory occupied by ND entries.

## Example

# Enable the device to learn the ND entry containing the link-local address of a peer interface.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] ipv6 nd link-local-entry-learn enable
```

# 6.10.44 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, the maximum of dynamic neighbor entries that an interface can learn is 212 for the S300, 1748 for the S500, 1000 for the SS1720GW-E, S1720GWR-E, S5720-LI, and S5720S-LI, 1024 for the S2730S-S, S5735-L-I, S5735-L1,S5735-L, S5735S-L, S5735S-L1, and S5735S-L-M, 2048 for the S5720I-SI, and 3072 for the S5735-S, S5735-S-I, and S5735S-S, 8192 for the S5731-S, S5731S-S, and 64000 for the 65536 for the S5731S-H and S5731-H, 10240 for the S5735S-H, S5736-S and 49152 for the S6720-EI, S6735-S and S6720S-EI, and 32768 for the S5732-H, S6730-S, S6730-H, S6730S-H, and S6730S-S.

## Format

**ipv6 nd neighbor-limit** *limit-number*

**undo ipv6 nd neighbor-limit**

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *limit-number* | Specifies the maximum number of dynamic neighbor entries that can be learned by a specified interface. | The value is an integer.<br>• The value ranges from 2 to 212 for the S300.<br>• The value ranges from 2 to 1748 for the S500.<br>• The value ranges from 2 to 1000 for the SS1720GW-E, S1720GWR-E, S5720-LI, and S5720S-LI.<br>• The value ranges from 2 to 1024 for the S2730S-S, S5735-L-I, S5735-L1,S5735-L, S5735S-L, S5735S-L1, and S5735S-L-M.<br>• The value ranges from 2 to 2048 for the S5720I-SI.<br>• The value ranges from 2 to 3072 for the S5735-S, S5735-S-I, and S5735S-S.<br>• The value ranges from 2 to 8192 for the S5731-S, and S5731S-S.<br>• The value ranges from 2 to 65536 for the S5731S-H and S5731-H.<br>• The value ranges from 2 to 10240 for the S5735S-H, S5736-S.<br>• The value ranges from 2 to 49152 for the S6720-EI, S6735-S and S6720S-EI.<br>• The value ranges from 2 to 32768 for the S5732-H, S6730-S, S6730S-S, S6730S-H, and S6730-H. |

## Views

VLANIF interface view, VBDIF 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
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 nd neighbor-limit 10
```

# 6.10.45 ipv6 nd ns multicast-enable

## Function

The **ipv6 nd ns multicast-enable** command enables a termination sub-interface to send NS multicast packets.

The **undo ipv6 nd ns multicast-enable** command disables a termination sub-interface from sending NS multicast packets.

By default, a termination sub-interface is disabled from sending NS multicast packets.

NOTE

Only S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

## Format

**ipv6 nd ns multicast-enable**

**undo ipv6 nd ns multicast-enable**

## Parameters

None

## Views

GE sub-interface view, XGE sub-interface view, MultiGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view, Eth-Trunk sub-interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

A termination sub-interface can send NS multicast packets to actively learn ND entries or respond to NS packets to passively learn ND entries.

When a 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 termination sub-interface to send NS multicast packets.

**Prerequisites**

Run the **ipv6 enable** command in the sub-interface view to enable IPv6 on a termination sub-interface.

Run the **dot1q termination vid** command in the sub-interface view to set the single VLAN ID for Dot1q termination. Or run the **qinq termination pe-vid ce-vid** command in the sub-interface view to configure a QinQ termination sub-interface to terminate double VLAN tags.

**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.

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.

VLAN termination sub-interfaces cannot be created on a VCMP client. You can run the **vcmp role** command to configure the role for a switch in a VCMP domain.

## Example

# Enable the Dot1q termination sub-interface GigabitEthernet0/0/1.1 to send NS multicast packets.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type hybrid
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] interface gigabitethernet 0/0/1.1
[HUAWEI-GigabitEthernet0/0/1.1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1.1] dot1q termination vid 100
[HUAWEI-GigabitEthernet0/0/1.1] ipv6 nd ns multicast-enable
```

# 6.10.46 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

## 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**

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 VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 nd ns retrans-timer 10000
```

# Set the interval for sending NS packets to 10000 milliseconds on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd ns retrans-timer 10000
```

# 6.10.47 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 30000 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 30000 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 CPU resources. Therefore, a short neighbor reachable time is not recommended on an IPv6 network. The default value, 30000 ms, is recommended.

If you run the **ipv6 nd nud reachable-time** command multiple times, only the latest configuration takes effect.

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 30000 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 30000 ms, the same as that on the device.

## Example

# Set the neighbor reachable time to 10000 ms on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 nd nud reachable-time 10000
```

# Set the neighbor reachable time to 10000 ms on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd nud reachable-time 10000
```

# 6.10.48 ipv6 nd proxy inner-access-vlan enable

## Function

The **ipv6 nd proxy inner-access-vlan enable** command enables intra-VLAN ND proxy on a VLANIF interface.

The **undo ipv6 nd proxy inner-access-vlan enable** command disables intra-VLAN ND proxy on a VLANIF interface.

By default, intra-VLAN ND proxy is disabled.

## Format

**ipv6 nd proxy inner-access-vlan enable**

**undo ipv6 nd proxy inner-access-vlan enable**

## Parameters

None

## Views

VLANIF interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Application Scenario**

On an IPv6 network, if port isolation is configured in a VLAN, users in the VLAN cannot communicate with each other. Configure intra-VLAN ND proxy on the VLAN-associated interface to enable Layer 3 communication among users.

**Prerequisites**

In the VLANIF interface view:

1. Run the **ipv6 enable** command to enable the IPv6 function.
1. Run the **ipv6 address** command to configure an IPv6 address for the interface. The IPv6 address must be in the same network segment as the IPv6 addresses of all hosts in the VLAN.

## Example

# Enable intra-VLAN ND proxy on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 address fc00::1/64
[HUAWEI-Vlanif100] ipv6 nd proxy inner-access-vlan enable
```

# 6.10.49 ipv6 nd proxy inter-access-vlan enable

## Function

The **ipv6 nd proxy inter-access-vlan enable** command enables inter-VLAN ND proxy on a VLANIF interface.

The **undo ipv6 nd proxy inter-access-vlan enable** command disables inter-VLAN ND proxy on a VLANIF interface.

By default, inter-VLAN ND proxy is disabled.

NOTE

Only the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S supports this command.

## Format

**ipv6 nd proxy inter-access-vlan enable**

**undo ipv6 nd proxy inter-access-vlan enable**

## Parameters

None

## Views

VLANIF interface view

## Default Level

2: Configuration level

## Usage Guidelines

### Application Scenario

In a VLAN aggregation scenario on an IPv6 network, if hosts in different sub-VLANs need to communicate at Layer 3, enable inter-VLAN ND proxy on the VLANIF interface corresponding to the super-VLAN. In this way, all sub-VLANs in the super-VLAN are reachable to each other.

### Prerequisites

In the VLANIF interface view:

1. Run the **ipv6 enable** command to enable the IPv6 function.
2. Run the **ipv6 address** command to configure an IPv6 address for the interface. The IPv6 address must be in the same network segment as the IPv6 addresses of all sub-VLAN hosts.

## Example

# Configure inter-VLAN ND proxy on VLANIF 30, the VLANIF interface corresponding to super-VLAN 30.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 30
[HUAWEI-Vlanif30] ipv6 enable
[HUAWEI-Vlanif30] ipv6 address fc00::1/64
[HUAWEI-Vlanif30] ipv6 nd proxy inter-access-vlan enable
```

# 6.10.50 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.

NOTE

If *min-interval* is not specified, the minimum interval varies depending on the maximum interval specified by *max-interval* (the minimum is 1/3 of the maximum). If *min-interval* is specified, the minimum interval is the value configured.

## Format

**ipv6 nd ra** { **max-interval** *maximum-interval* | **min-interval** *minimum-interval* }

**undo ipv6 nd ra** { **max-interval** | **min-interval** }

## 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.<br>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. To reduce the number of RA messages being transmitted on a link, you can set a longer interval. To speed up router discovery, you can set a shorter interval.

### 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 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.

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 VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 nd ra max-interval 1000
```

# Set the maximum interval for sending RA packets to 1000s on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd ra max-interval 1000
```

# Set the minimum interval for sending RA packets to 300s on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 nd ra min-interval 300
```

# Set the minimum interval for sending RA packets to 300s on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd ra min-interval 300
```

## 6.10.51 ipv6 nd ra dns-server

### Function

The **ipv6 nd ra dns-server** command configures a DNS server address for RA packets.

The **undo ipv6 nd ra dns-server** command deletes the DNS server address configured for RA packets.

By default, RA packets do not contain a DNS server address.

### Format

**ipv6 nd ra dns-server** *ipv6-address* [ *valid-lifetime* ]

**undo ipv6 nd ra dns-server** [ *ipv6-address* [ *valid-lifetime* ] ]

### Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *ipv6-address* | Specifies the IPv6 address of a DNS server. | 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. |
| *valid-lifetime* | Specifies a valid lifetime. | The value is an integer ranging from 1 to 4294967295, in seconds. The default value is three times the maximum interval for advertising RA packets. The maximum interval for advertising RA packets can be configured using the **ipv6 nd ra max-interval** *maximum-interval* command. |

### Views

Interface view

### Default Level

2: Configuration level

## Usage Guidelines

### Usage Scenario

In a scenario where IPv6 ND stateless address auto-configuration is used or DHCPv6 is not configured, run the **ipv6 nd ra dns-server** command to configure a DNS server address for RA packets so that the host can implement the DNS service using the DNS server address in RA packets.

### Prerequisites

The IPv6 function has been enabled on an interface using the **ipv6 enable** command in the interface view.

### Precautions

A maximum of eight DNS server addresses can be configured for the RA packets transmitted on the same interface.

## Example

# Configure a DNS server address for the RA packets transmitted on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd ra dns-server 2001:db8:1::2 1000
```

# 6.10.52 ipv6 nd ra dns-suffix

## Function

The **ipv6 nd ra dns-suffix** command sets a DNS suffix in RA packets.

The **undo ipv6 nd ra dns-suffix** command deletes the DNS suffix configured for RA packets.

By default, RA packets do not contain a DNS suffix.

## Format

**ipv6 nd ra dns-suffix** *domain-suffix* [ *valid-lifetime* ]

**undo ipv6 nd ra dns-suffix** [ *domain-suffix* [ *valid-lifetime* ] ]

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *domain-suffix* | Specifies a DNS suffix. | The value is a string of 1 to 64 characters and can contain digits, letters, hyphens (-), underscores (_), and periods (.), but not spaces. |

| Parameter | Description | Value |
| --- | --- | --- |
| *valid-lifetime* | Specifies a valid lifetime. | The value is an integer ranging from 1 to 4294967295, in seconds. The default value is three times the maximum interval for advertising RA packets. The maximum interval for advertising RA packets can be configured using the **ipv6 nd ra max-interval** *maximum-interval* command. |

## Views

Interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

To allow a host use a DNS domain name with a suffix upon receipt of RA packets, run the **ipv6 nd ra dns-suffix** command to configure a DNS suffix for RA packets.

**Prerequisites**

The IPv6 function has been enabled on an interface using the **ipv6 enable** command in the interface view.

**Precautions**

Only one DNS suffix can be configured for the RA packets transmitted on the same interface. If the **ipv6 nd ra dns-suffix** command is run more than once for the same interface, the latest configuration overrides the previous one.

## Example

# Configure a DNS suffix for the RA packets transmitted on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd ra dns-suffix example.com 1000
```

# 6.10.53 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**

- 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 in the interface view using the **ipv6 enable** command.

**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.

You can run the **display icmpv6 statistics** command to check whether a local device has sent RA packets.

## Example

# Disable VLANIF100 from sending RA packets.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 nd ra halt
```

# Disable GE0/0/1 from sending RA packets.

```
<HUAWEI> system-view
[HUAWEI] ipv6
```

```
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd ra halt
```

# 6.10.54 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**

## 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 switch, 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 VLANIF100 to 126.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 nd ra hop-limit 126
```

# Set the hop limit for RA packets sent by GE0/0/1 to 126.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd ra hop-limit 126
```

# 6.10.55 ipv6 nd ra preference

## Function

The **ipv6 nd ra preference** command configures the default router priority value in the RA packets.

The **undo ipv6 nd ra preference** command restores the default router priority value in RA packets to be the default value.

By default, the router priority of RA packets is medium.

## Format

**ipv6 nd ra preference** { **high** | **medium** | **low** }

**undo ipv6 nd ra preference**

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **high** | Specifies the default router priority to be high. | - |
| **medium** | Specifies the default router priority to be medium. | - |
| **low** | Specifies the default router priority to be low. | - |

## Views

Interface view

## Default Level

2: Configuration level

## Usage Guidelines

### Usage Scenario

If there are multiple switches on the links connected to a host, the host needs to select suitable switches based on different destination addresses of the packets to be forwarded. Each switch advertises its default router priority and specific route information to the host so that the host can enhance its own capability of selecting suitable forwarding switches based on different IP addresses of the packets to be forwarded.

After receiving an RA message that contains the default router priority, the host updates its own default router list. If the host does not have any route to select when sending packets to other devices, the host will search the updated router list for the switch with the highest priority. If the switch with the highest priority becomes faulty, the host selects another switch in descending order of priority.

To set a default router priority in RA messages, run the **ipv6 nd ra preference** command. This setting allows the switch with the highest priority to function as the gateway for hosts.

### Prerequisites

Before running this command, run the **ipv6 enable** command on the interface view to enable the IPv6 function.

By default, the switch does not advertise RA packets. Therefore, to allow the default router priority to be advertised to the host, you need to run the **undo ipv6 nd ra halt** command to enable the function of advertising RA packets for the device.

### Precautions

If the system is deleting the binding relationship between an interface and an IPv6 address family VPN instance, you are prompted not to run the **ipv6 nd ra preference** command.

## Example

# Configure the default router priority value in RA packets on VLANIF100 to be high.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] undo ipv6 nd ra halt
[HUAWEI-Vlanif100] ipv6 nd ra preference high
```

# Configure the default router priority value in RA packets on GE0/0/1 to be high.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
```

```
[HUAWEI-GigabitEthernet0/0/1] undo ipv6 nd ra halt
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd ra preference high
```

# 6.10.56 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. |
| *prefix-length* | Specifies the prefix length of an IPv6 address. | The value is an integer that ranges from 0 to 128. You can calculate the IPv6 prefix carried in the RA packet based on the IPv6 address and prefix length. When stateless autoconfiguration is used, specify the length of address prefix as 64; otherwise, the address will be invalid and RA packets are discarded. |

| Parameter | Description | Value |
| --- | --- | --- |
| *valid-lifetime* | Specifies the valid lifetime of the prefix.<br>The valid lifetime decides the prefix on-link status. | The value is an integer that ranges from 0 to 4294967295, in seconds. |
| *preferred-lifetime* | Specifies the preferred lifetime of the prefix. The length of time in seconds (relative to the time the packet is sent) that addresses generated from the prefix via stateless address autoconfiguration remain preferred.<br>The preferred lifetime cannot be larger than the valid lifetime. | The value is an integer that ranges from 0 to 4294967295, in seconds. |
| **no-autoconfig** | Deletes the A-Flag. If **no-autoconfig** is specified, a configured prefix cannot be used in stateless address allocation.<br>A-Flag indicates the autonomous address configuration in the prefix option of RA packet. | - |
| **off-link** | Specifies the L-Flag. If **off-link** is specified, indicates that this prefix can be used for on-link determination. When **off-link** is not specified, the advertisement makes no statement about on-link or off-link properties of the prefix. In other words, if the L flag is not set a host MUST NOT conclude that an address derived from the prefix is off-link. That is, it MUST NOT update a previous indication that the address is on-link. | - |
| **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**

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 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).

The prefix configuring using the **ipv6 nd ra prefix** command takes precedence over the default prefix generated based on the interface IPv6 address. An RA message can carry a maximum of 10 prefixes. If exactly 10 prefixes have been manually configured, the default prefix will not be carried.

In the DHCPv6 stateful address autoconfiguration scenario, the lifetime of the PD prefixes advertised in RA packets is the default value defined in DHCPv6. If the prefixes in RA packets remain unchanged, you can run the **ipv6 nd ra prefix** command to configure static prefixes and specify their lifetime. If the prefixes in RA packets change, you need to specify the lifetime of the changed prefixes.

## Example

# Configure the prefix in the RA packet on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] undo ipv6 nd ra halt
[HUAWEI-Vlanif100] ipv6 nd ra prefix fc00:1::100 128 1000 400 no-autoconfig
[HUAWEI-Vlanif100] ipv6 nd ra prefix fc00:2::100 64 1000 400 off-link
```

# Configure the prefix in the RA packet on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] undo ipv6 nd ra halt
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd ra prefix fc00:1::100 128 1000 400 no-autoconfig
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd ra prefix fc00:2::100 64 1000 400 off-link
```

# Configure RA packets on VLANIF100 not to carry the default prefix.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] undo ipv6 nd ra halt
[HUAWEI-Vlanif100] ipv6 nd ra prefix default no-advertise
```

# 6.10.57 ipv6 nd ra route-information

## Function

The **ipv6 nd ra route-information** command configures route information in RA packets.

The **undo ipv6 nd ra route-information** command deletes route information in RA packets.

By default, there is no route information in RA packets.

## 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 IPv6 address. | The prefix is a 32-bit hexadecimal number, in the format of 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 lifetime of a route. | The value is an integer ranging from 0 to 4294967295, in seconds. |
| **preference** | Specifies the priority of a route. | - |
| **high** | Specifies the route priority to be high. | - |
| **medium** | Specifies the route priority to be medium. | - |
| **low** | Specifies the route priority to be low. | - |

## Views

Interface view

## Default Level

2: Configuration level

## Usage Guidelines

### Usage Scenario

An RA packet includes route information. The switch sends the specified routes to the hosts on the local network segment by using this information. The hosts can send packets by using these routes.

When receiving the RA packets carrying route information, a host updates its routing table. When sending the RA packets to another device, a host queries the routing table and selects proper route for sending packets.

### Prerequisites

Before running this command, run the **ipv6 enable** command on the interface view to enable the IPv6 function of an interface.

By default, the switch does not send RA packets. Therefore, to send the routes to the host, you need to run the **undo ipv6 nd ra halt** command to enable the function of advertising RA packets for the device.

### Precautions

A maximum of 17 route options are supported on each interface.

When this command is to be run, the value of *ipv6-address* cannot be a loopback address.

## Example

# Configure the route information of RA packets on VLANIF100: The lifetime of the route with the destination address of 2001:db8::2/64 is 1550 seconds, and the priority of this route is high.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] undo ipv6 nd ra halt
[HUAWEI-Vlanif100] ipv6 nd ra route-information 2001:db8::2 64 lifetime 1550 preference high
```

# Configure the route information of RA packets on GE0/0/1: The lifetime of the route with the destination address of 2001:db8::2/64 is 1550 seconds, and the priority of this route is high.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] undo ipv6 nd ra halt
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd ra route-information 2001:db8::2 64 lifetime 1550 preference
high
```

# 6.10.58 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 of an RA packet is 1800s.

## Format

**ipv6 nd ra router-lifetime** *ra-lifetime*

**undo ipv6 nd ra router-lifetime**

## 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. The default value is 1800 seconds, which is recommended. |

## 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.

**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 switch to its default router table.

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 VLANIF100 to 1000s.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 nd ra router-lifetime 1000
```

# Set the lifetime of the RA packets on GE0/0/1 to 1000s.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd ra router-lifetime 1000
```

# 6.10.59 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.

## 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, 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 IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

**Precautions**

If the aging time is not configured on an interface, the aging time configured in system view is used for the interface. If the aging time is configured on an interface, the interface configuration takes effect.

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. That is, the new aging time configuration takes effect after the last aging time 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.

## Example

# Set the aging time of ND entries in STALE state to 3600s on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 nd stale-timeout 3600
```

# Set the aging time of ND entries in STALE state to 3600s on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 nd stale-timeout 3600
```

# 6.10.60 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

VLANIF interface view:

**ipv6 neighbor** *ipv6-address mac-address* **vid** *vlan-id interface-type interface-number*

**undo ipv6 neighbor** *ipv6-address*

Ethernet interface view, Eth-Trunk interface view, Ethernet sub-interface view, and Eth-Trunk sub-interface view:

**ipv6 neighbor** *ipv6-address mac-address* [ **vid** *vlan-id* [ **cevid** *cevid* ] ]

**undo ipv6 neighbor** *ipv6-address*

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the command in Ethernet interface view and Ethernet sub-interface view.

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *ipv6-address* | Specifies the IPv6 address of a static neighbor entry. | 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. |
| *mac-address* | Specifies the MAC address of a static neighbor entry. | The value is in the H-H-H format. An H contains one to four hexadecimal numbers. |
| **vid** *vlan-id* | Specifies the ID of the outer VLAN to which the interface belongs. | The value is an integer that ranges from 1 to 4094. |
| **cevid** *cevid* | Specifies the ID of the inner VLAN to which the interface belongs. | 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**

To filter invalid packets, you can create static neighbor entries, binding the destination IPv6 addresses of these packets to nonexistent MAC addresses.

**Prerequisites**

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

**Precautions**

A neighbor entry enters the REACHABLE state after being created, indicating that the interface connected to this neighbor is Up.

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 VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 neighbor fc00::1 00e0-fc12-3456 vid 2 gigabitethernet 0/0/1
```

# Configure static neighbor entries on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 neighbor fc00::1 00e0-fc12-3456
```

# 6.10.61 ipv6 packet-too-big drop

## Function

The **ipv6 packet-too-big drop** configures the switch to discard packets with the length larger than the IPv6 MTU of the outbound interface, and enables IPv6 PMTU discovery.

The command **undo ipv6 packet-too-big drop** restores the default policy for processing packets with the length larger than the IPv6 MTU of the outbound interface.

By default, the switch properly forwards packets with the length larger than the IPv6 MTU of the outbound interface and IPv6 PMTU discovery is disabled.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

## Format

**ipv6 packet-too-big drop**

**undo ipv6 packet-too-big drop**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

When the switch functions as an intermediate node on an IPv6 network, you can configure the **ipv6 packet-too-big drop** command to discard packets with the length larger than the IPv6 MTU of the outbound interface and enable IPv6 PMTU discovery.

In an IPv4 network, oversized packets need to be fragmented. When a transit device receives a packet exceeding the maximum transmission unit (MTU) size of its outbound interface from a source node, the transit device fragments the packet before forwarding it to the destination node. In an IPv6 network, however, only the source node can fragment packets, which reducing pressure on transit devices. When an interface on a transit device receives a packet whose size exceeds the MTU, the transit device discards the packet and sends an ICMPv6 Packet Too Big message to the source node. The ICMPv6 Packet Too Big message contains the MTU value of the outbound interface. The source node fragments the packet based on the MTU and resends the packet, increasing traffic overhead. The Path MTU Discovery protocol dynamically discovers the MTU value of each link on the transmission path, reducing excessive traffic overhead.

The PMTU Discovery protocol is implemented through ICMPv6 Packet Too Big messages. A source node first uses the MTU of its outbound interface as the PMTU and sends a probe packet. If a smaller PMTU exists on the transmission path, the transit device sends a Packet Too Big message to the source node. The Packet Too Big message contains the MTU value of the outbound interface on the transit device. After receiving this message, the source node changes the PMTU value to the received MTU value and sends packets based on the new MTU. This process repeats until packets are sent to the destination address. The source node obtains the PMTU of the destination address.

**Precautions**

The switch supports IPv6 MTU discovery, but does not support IPv6 packet fragmentation when it functions as an intermediate node. IPv6 packets can be fragmented only on source nodes.

## Example

# Configure the switch to discard packets with the length larger than the IPv6 MTU of the interface, and enable IPv6 PMTU discovery.

```
<HUAWEI> system-view
[HUAWEI] ipv6 packet-too-big drop
Warning: This operation will affect IPv6 traffic forwarding. Continue? [Y/N]:y
```

# 6.10.62 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.<br>**NOTE**<br>The link-local address does not take effect. | 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 name. |
| *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 recommended 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
```

# 6.10.63 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.

## Example

# Set the aging time of dynamic PMTU entries to 40 minutes.

```
<HUAWEI> system-view
[HUAWEI] ipv6 pathmtu age 40
```

# 6.10.64 nd optimized-passby enable

## Function

The **nd optimized-passby enable** command configures the device not to send NS packets destined for other devices to the CPU.

The **undo nd optimized-passby enable** command configures the device to send NS packets destined for other devices to the CPU.

By default, a device does not send NS packets destined for other devices to the CPU.

## Format

**nd optimized-passby enable**

**undo nd optimized-passby enable**

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

## Parameters

None

## Views

VLANIF interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

If an interface receives a large number of NS packets whose destination IPv6 addresses are different from the IPv6 address of this interface and sends these NS packets to the CPU for processing, the CPU usage is high and the CPU cannot process services properly.

To prevent this issue, you can configure the device to directly forward NS packets destined for other devices without sending them to the CPU. This improves the device's capability of defending against packet attacks.

**Precautions**

If the **nd snooping enable** is executed in system view, or if IPv6 protocol is **Down** on the VLANIF interface, the configuration of disabling the device from sending NS packets destined for other devices to the CPU does not take effect on the VLANIF interface.

## Example

# Configure the device to send NS packets destined for other devices to the CPU.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] undo nd optimized-passby enable
```

# 6.10.65 nd optimized-reply disable

## Function

The **nd optimized-reply disable** command disables the optimized ND reply function.

The **undo nd optimized-reply disable** command enables the optimized ND reply function.

By default, the optimized ND reply function is enabled.

## Format

**nd optimized-reply disable**

**undo nd optimized-reply disable**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

When a stack functions as an access gateway, it receives a large number of ND Request packets that request the switch to reply with its local interface MAC address. If all these ND Request packets are sent to the master switch, the CPU usage of the master switch increases, and other services are affected.

The optimized ND reply function addresses this issue. After this function is enabled, the switch receiving an ND Request packet returns an ND Reply packet if the ND Request packet is destined for a local interface on the switch of the stack, and discards the ND Request packet if the packet is not destined for a local interface on the switch of the stack.

By default, the optimized ND reply function is enabled. After receiving an ND Request packet, the switch checks whether an ND entry corresponding to the source IPv6 address of the ND Request packet exists.

- If the corresponding ND entry exists and the packet information is the same as the saved ND entry information, the switch performs optimized ND reply to this ND Request packet.
- If the corresponding ND entry exists but the packet information differs from the saved ND entry information, the switch does not perform optimized ND reply to this ND Request packet.
- If the corresponding ND entry does not exist, the switch does not perform optimized ND reply to this ND Request packet.

**Precautions**

- The optimized ND reply function takes effect for ND Request packets sent by wireless users.

- The optimized ND reply function takes effect for ND Request packets received on VLANIF interfaces and VBDIF interfaces enabled with IPv6. VLANIF interfaces of Group VLANs and Separate VLANs in MUX VLANs, VLANIF interfaces of mapped VLANs, and VLANIF interfaces of super-VLANs do not perform optimized ND reply.
- If the number of global unicast IPv6 addresses on a VLANIF interface or VBDIF interface enabled with IPv6 exceeds 1, the switch does not perform optimized ND reply for NS packets received on this interface.
- If the ND snooping function is enabled on a switch, the switch does not perform optimized ND reply to received ND Request packets.
- The switch does not perform optimized ND reply to the following received packets:
  - NS packets with the source IPv6 address :: (that is, Duplicate Address Detection packets)
  - Packets with IPv6 extension headers

## Example

# Disable the optimized ND reply function.

```
<HUAWEI> system-view
[HUAWEI] nd optimized-reply disable
```

# 6.10.66 nd trap hash-conflict enable

## Function

The **nd trap hash-conflict enable** command enables the trap function for hash conflicts of ND entries.

The **undo nd trap hash-conflict enable** command disables the trap function for hash conflicts of ND entries.

By default, the trap function for hash conflicts of ND entries is enabled.

## Format

**nd trap hash-conflict enable**

**undo nd trap hash-conflict enable**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

After the trap function for hash conflicts of ND entries is configured, the switch sends traps when a hash conflict of ND entries occurs so that you can obtain the status of ND entries promptly. ND entry resources are key resources on the switch. Monitoring the ND entry status effectively ensures proper running of the switch.

To improve the IPv6 forwarding performance, the switch saves ND entries using hash links. When multiple ND entries obtain the same key based on the hash algorithm, the ND entries cannot be saved. This is a hash conflict of ND entries.

When a hash conflict of ND entries occurs, the switch has available ND entry space but cannot save ND entries. The switch cannot forward IPv6 traffic matching the ND entries with a hash conflict.

You can enable the trap function for hash conflicts of ND entries to detect hash conflicts of ND entries promptly.

## Example

# Enable the trap function for hash conflicts of ND entries.

```
<HUAWEI> system-view
[HUAWEI] nd trap hash-conflict enable
```

# 6.10.67 nd trap hash-conflict history

## Function

The **nd trap hash-conflict history** command sets the number of traps reported within each interval when a hash conflict of ND entries occurs.

The **undo nd trap hash-conflict history** command restores the default number of traps reported within each interval when a hash conflict of ND entries occurs.

By default, a switch reports a maximum of 10 traps within each interval when a hash conflict of ND entries occurs.

## Format

**nd trap hash-conflict history** *history-number*

**undo nd trap hash-conflict history**

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *history-number* | Specifies the number of traps reported within each interval when a hash conflict of ND entries occurs. | The value is an integer that ranges from 10 to 30. The default value is 10. |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

After the trap function for hash conflicts of ND entries is enabled, the switch reports a maximum of 10 traps within 60 seconds by default. Each trap contains an IPv6 address that has a hash conflict.

If hash conflicts of more than 10 ND entries occur within an interval, traps for the eleventh and following ND entries that have hash conflicts cannot be reported. To solve this problem, you can run the **nd trap hash-conflict history** command to set the number of traps reported within each interval when a hash conflict of ND entries occurs.

**Precautions**

If you run this command multiple times, only the latest configuration takes effect.

## Example

# Configure the switch to report a maximum of 15 traps within each interval when a hash conflict of ND entries occurs.

```
<HUAWEI> system-view
[HUAWEI] nd trap hash-conflict history 15
```

# 6.10.68 nd trap hash-conflict interval

## Function

The **nd trap hash-conflict interval** command sets the interval at which the switch reports traps when a hash conflict of ND entries occurs.

The **undo nd trap hash-conflict interval** command restores the default interval at which the switch reports traps when a hash conflict of ND entries occurs.

By default, a switch reports traps at an interval of 60 seconds when a hash conflict of ND entries occurs.

## Format

**nd trap hash-conflict interval** *interval-time*

**undo nd trap hash-conflict interval**

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *interval-time* | Specifies the interval at which the switch reports traps when a hash conflict of ND entries occurs. | The value is an integer that ranges from 30 to 3600, in seconds. The default value is 60. |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

After the trap function for hash conflicts of ND entries is enabled, the switch reports a maximum of 10 traps within 60 seconds by default. Each trap contains an IPv6 address that has a hash conflict.

If the trap report interval is set to a small value, the switch reports traps for hash conflicts of ND entries more promptly. When many hash conflicts of ND entries occur, the switch reports a lot of traps.

If the trap report interval is set to a large value, the switch reports traps for hash conflicts of ND entries less promptly. When many hash conflicts of ND entries occur, the switch suppresses traps to be reported.

You can run the **nd trap hash-conflict interval** command to adjust the trap report interval based on actual requirements.

**Precautions**

If you run this command multiple times, only the latest configuration takes effect.

## Example

# Configure the switch to report traps at an interval of 90 seconds when a hash conflict of ND entries occurs.

```
<HUAWEI> system-view
[HUAWEI] nd trap hash-conflict interval 90
```

# 6.10.69 nd-miss message-cache disable

## Function

The **nd-miss message-cache disable** command disables the ND Miss message sending function.

The **undo nd-miss message-cache disable** command enables the ND Miss message sending function.

By default, the ND Miss message sending function is enabled.

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

## Format

**nd-miss message-cache disable**

**undo nd-miss message-cache disable**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

If a user sends an IPv6 packet with an irresolvable destination IPv6 address to the device (that is, if the device has a route to the destination IPv6 address of the IPv6 packet but has no ND entry matching the next hop of the route), the device generates an ND Miss message. By default, the device sends the ND Miss messages to the CPU. This improves the efficiency of processing the ND Miss messages.

When the ND Miss message sending function is enabled, a device cannot reply to ICMPv6 host unreachable packets. To enable the device to reply to ICMPv6 host unreachable packets, you can run the **nd-miss message-cache disable** command to disable the ND Miss message sending function.

## Example

# Disable the ND Miss message sending function.

```
<HUAWEI> system-view
[HUAWEI] nd-miss message-cache disable
```

# 6.10.70 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

2: Configuration 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
```

# 6.10.71 reset ipv6 neighbors

## Function

The **reset ipv6 neighbors** command clears neighbor entries.

## 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.<br>The second **dynamic** indicates that dynamic neighbor entries on the current interface are cleared. | - |

| Parameter | Description | Value |
| --- | --- | --- |
| **static** | The first **static** indicates that static neighbor entries on all interfaces are cleared.<br>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.<br>• *interface-type* specifies the interface type.<br>• *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

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 the specified interface VlANIF 10.

```
<HUAWEI> reset ipv6 neighbors vlanif 10
```

# 6.10.72 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 name. |

## Views

User view

## Default Level

3: Management level

## Usage Guidelines

**Usage Scenario**

To collect statistics on PMTU entries within a specified period, use the **reset ipv6 pathmtu** command to clear the existing statistics on PMTU entries before running the **display ipv6 pathmtu** command to check information about PMTU entries.

**Precautions**

The **reset ipv6 pathmtu all** 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, continue?[Y/N]:y
```

# 6.10.73 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 and the range depends on the task configuration. |
| **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.

## 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
```

# 6.10.74 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
```

# 6.10.75 reset nd optimized-reply statistics

## Function

The **reset nd optimized-reply statistics** command clears statistics on optimized ND Reply packets.

## Format

**reset nd optimized-reply statistics** [ **slot** *slot-id* ]

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **slot** *slot-id* | Specifies the stack ID. | The value is an integer. It has a fixed value of 0 in a non-stack scenario, and depends on the device configuration in a stack scenario. |

## Views

User view

## Default Level

2: Configuration level

## Usage Guidelines

Before collecting statistics on optimized ND Reply packets on the device, you can run the **reset nd optimized-reply statistics** command to clear statistics on optimized ND Reply packets of the device.

## Example

# Clears statistics on optimized ND Reply packets.

```
<HUAWEI> reset nd optimized-reply statistics
```

# 6.10.76 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
```

# 6.10.77 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
```

# 6.10.78 reset tcp ipv6 statistics

## Function

The **reset tcp ipv6 statistics** command clears TCP6 packet statistics.

## Format

**reset tcp ipv6 statistics**

## Parameters

None

## Views

User view

## Default Level

3: Management level

## Usage Guidelines

**Usage Scenario**

To delete TCP6 packet statistics displayed using the **display tcp ipv6 statistics** command, run the **reset tcp ipv6 statistics** command. The TCP6 packet statistics include the number of both sent and received packets, the number of discarded packets, the number of redirected packets, the threshold-crossing status of TCP6 connections, network attack status, and network quality. You can run the **reset tcp ipv6 statistics** command to delete existing statistics and then run the **display tcp ipv6 statistics** command to collect statistics. The statistics help you check whether TCP6 packet counts are correct or help you diagnose faults.

**Precautions**

The **reset tcp ipv6 statistics** command clears TCP6 packet statistics. Therefore, confirm your action before running this command.

## Example

# Clear TCP6 packet statistics.

```
<HUAWEI> reset tcp ipv6 statistics
```

# 6.10.79 reset udp ipv6 statistics

## Function

The **reset udp ipv6 statistics** command clears UDP6 packet statistics.

## Format

**reset udp ipv6 statistics**

## Parameters

None

## Views

User view

## Default Level

3: Management level

## Usage Guidelines

**Usage Scenario**

To delete UDP6 packet statistics displayed using the **display udp ipv6 statistics** command, run the **reset udp ipv6 statistics** command. The statistics include the number of both the sent and received packets, the number of discarded packets, and the number of redirected packets. You can run the **reset udp ipv6 statistics** command to delete existing statistics and then run the **display udp ipv6 statistics** command to collect statistics. The statistics help you check whether UDP6 packet counts are correct or help you diagnose faults.

**Precautions**

The **reset udp ipv6 statistics** command clears UDP6 packet statistics. Therefore, confirm your action before running this command.

## Example

# Clear UDP6 packet statistics.

```
<HUAWEI> reset udp ipv6 statistics
```

# 6.10.80 segment-routing ipv6 head pop

## Function

The **segment-routing ipv6 head pop** command enables SRv6 packet decapsulation.

The **undo segment-routing ipv6 head pop** command disables SRv6 packet decapsulation.

By default, SRv6 packet decapsulation is disabled.

**NOTE**

This command is supported only on the following models:
S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S

## Format

**segment-routing ipv6 head pop**

**undo segment-routing ipv6 head pop**

## Parameters

None

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

Segment Routing over IPv6 (SRv6) is designed to forward IPv6 packets on a network through source routing. SRv6 is based on the IPv6 forwarding plane. With SRv6, a segment routing header (SRH) is added to IPv6 packets. If the downstream device of a switch cannot process SRv6 packets, run the **segment-routing ipv6 head pop** command on the switch to enable SRv6 packet decapsulation and then configure MQC- or ACL-based redirection. In this case, the switch will forward the decapsulated IPv6 packets to the downstream device.

The following actions are taken to decapsulate SRv6 packets:

- Change the value in the **Next Header** field in the IPv6 header to the value in the **Next Header** field in the SRH.
- Change the value in the **Destination Address** field in the IPv6 header to the first IPv6 address (that is, segment list [0]) in the SRH.
- Remove the SRH from the packet.
- Subtract the SRH length from the **Payload Length** field in the IPv6 header.

**Follow-up Procedure**

Configure MQC- or ACL-based redirection to redirect decapsulated packets to other devices.

**Precautions**

After the **segment-routing ipv6 head pop** command is run, SRv6 packets cannot be mirrored or sampled, or sent to the CPU.

## Example

# Enable SRv6 packet decapsulation.

```
<HUAWEI> system-view
[HUAWEI] segment-routing ipv6 head pop
```

# 6.10.81 service type tunnel

## Function

The **service type tunnel** command enables service loopback on an Eth-Trunk interface to loop service packets back to tunnel interfaces.

The **undo service type tunnel** command disables service loopback on an Eth-Trunk interface.

By default, service loopback is disabled on an Eth-Trunk interface.

NOTE

Only the S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

## Format

**service type tunnel**

**undo service type tunnel**

## Parameters

None

## Views

Eth-Trunk interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

To forward packets using tunnel interfaces, you need to bind the tunnel interfaces to an Eth-Trunk interface. Before binding the tunnel interfaces to the Eth-Trunk interface, run the **service type tunnel** command to enable service loopback on the Eth-Trunk interface to loop service packets back to tunnel interfaces.

**Precautions**

After being configured as a service loopback interface, an Eth-Trunk interface can only be used to loop service packets back to tunnel interfaces.

A device can be configured with only one service loopback interface.

You cannot configure both the **service type tunnel** command and the URPF function on the same Eth-Trunk.

On an Eth-Trunk enabled with the service loopback function, the STP function is automatically disabled. After the service loopback function is disabled on the Eth-Trunk, the STP function is automatically enabled.

- The configurations allowed on an Eth-Trunk to be configured as a loopback interface include **description**, **enable snmp trap updown**, **jumboframe enable**, **mixed-rate link enable**, **qos phb marking enable**, **set flow-stat interval**, **shutdown**, **local-preference enable**, **traffic-policy (interface view)**, and **trust**. If other configurations exist on the Eth-Trunk, the Eth-Trunk cannot be configured as a loopback interface.
- After an Eth-Trunk is configured as a loopback interface, the Eth-Trunk supports only the following configurations: **authentication open ucl-policy enable**, **description**, **enable snmp trap updown**, **jumboframe enable**, **mixed-rate link enable**, **qos phb marking enable**, **set flow-stat interval**, **shutdown**, **local-preference enable**, **statistic enable (interface view)**, **traffic-policy (interface view)**, **vcmp disable**, and **trust**.
- Before running the **undo service type tunnel** command, delete all the member interfaces of the Eth-Trunk interface on the device.

After the Eth-Trunk interface is configured as the service loopback interface, other service configurations cannot be performed on the Eth-Trunk interface by invoking the MIB through the NMS. Otherwise, the service loopback interface function or the service configurations delivered through the MIB may be invalid.

## Example

# Enable service loopback on the interface **Eth-Trunk 0**.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 0
[HUAWEI-Eth-Trunk0] service type tunnel
```

# 6.10.82 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.

## 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
```

# 6.10.83 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.

## 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 bytes 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) 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**

The minimum MSS value configured using the **tcp ipv6 min-mss** command must be less than the maximum MSS value configured using the **tcp ipv6 max-mss** command.

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
```

# 6.10.84 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 600s.

## 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 600s. |

## Views

System view

## Default Level

2: Configuration level

## 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
```

# 6.10.85 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. |

## 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
```

# 6.10.86 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**

## 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
```

# 6.11 DHCPv6 Configuration Commands

## 6.11.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

Layer 3 Ethernet interface, VLANIF interface, and sub-interface all support the DHCPv6 function.

## 6.11.2 address prefix

### Function

The **address prefix** command configures the network prefix and lifetime in the IPv6 address pool view.

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** *ipv6-prefix/ipv6-prefix-length* [ **eui-64** ] [ **life-time** { *valid-lifetime* | **infinite** } { *preferred-lifetime* | **infinite** } ]

**address prefix** *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** *ipv6-prefix/ipv6-prefix-length* [ **lock** ]

**undo address prefix** *ipv6-prefix/ipv6-prefix-length* [ **lock** ]

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *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.<br>*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. | - |
| *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.<br>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.<br>When the preferred lifetime is set to infinite, the valid lifetime must be set to infinite. | - |

| 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.<br>• *hours*: indicates hours. The value is an integer that ranges from 0 to 23.<br>• *minutes*: indicates minutes. The value is an integer that ranges from 0 to 59.<br>• *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.<br>• *hours*: indicates hours. The value is an integer that ranges from 0 to 23.<br>• *minutes*: indicates minutes. The value is an integer that ranges from 0 to 59.<br>• *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).

**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
```

# 6.11.3 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

## 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 **dhcpv6 pool** command.

**Precautions**

You can run the **capwap-ac** command multiple times to configure the IPv6 addresses of several ACs, and the AC's IPv6 address 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
```

# 6.11.4 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**

## 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
```

# 6.11.5 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.

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

VLANIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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 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 **ipv6** command in the system view.
2. IPv6 functions have been enabled on interfaces using the **ipv6 enable** 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.

## Example

# Configure the DHCPv6 client to obtain configuration parameters using stateless DHCPv6 address autoconfiguration on the interface VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 address auto link-local
[HUAWEI-Vlanif100] dhcpv6 client information-request
```

# Configure the DHCPv6 client to obtain configuration parameters using stateless DHCPv6 address autoconfiguration on the interface

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 address auto link-local
[HUAWEI-GigabitEthernet0/0/1] dhcpv6 client information-request
```

# 6.11.6 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 pd** *prefix-name* [ **hint** *ipv6-prefix/ipv6-prefix-length* ] [ **rapid-commit** ] [ **unicast-option** ]

**undo dhcpv6 client pd**

## 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. |
| **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.<br>*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. | - |

## Views

VLANIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

## Default Level

2: Configuration level

## 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 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 **ipv6** command in the system view.
2. IPv6 functions have been enabled on interfaces using the **ipv6 enable** 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 VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 address auto link-local
[HUAWEI-Vlanif100] dhcpv6 client pd example
```

# Configure the DHCPv6 PD client to obtain IPv6 address prefix using stateless DHCPv6 address autoconfiguration on the interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 address auto link-local
[HUAWEI-GigabitEthernet0/0/1] dhcpv6 client pd example
```

# 6.11.7 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

VLANIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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 vlanif 100
[HUAWEI-Vlanif100] ipv6 address auto dhcp
[HUAWEI-Vlanif100] dhcpv6 client renew
```

# Manually update the applied IPv6 prefix.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcpv6 client pd myprefix
[HUAWEI-Vlanif100] dhcpv6 client renew
```

# 6.11.8 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* }

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **ll** | Configures the device to generate a DUID based on the link-layer address (MAC address). | - |

| Parameter | Description | Value |
| --- | --- | --- |
| **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
```

# 6.11.9 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.<br>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 00e0-fc12-3456, the Interface-ID generated during the system parsing process is 0011.0022.00e0fc123456:vlanif100. | - |
| **user-defined** *text* | Specifies a user-defined format as the Interface-ID format. A user-defined format can be:<br>• 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.<br>For description of the keywords supported by the user-defined format, see **Table 6-76**.<br>• 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.<br>• 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.

**Table 6-76** 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. |

| Keyword | Description |
| --- | --- |
| 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.
- 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"
```

# 6.11.10 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.

NOTE

This command is supported only on the following models: S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S5720S-LI, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731S-H, S5731-S, S5731S-S, S6735-S, S6720-EI, S6720S-EIS5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S, S6720S-S.

## Format

**dhcpv6 interface-id insert enable**

**undo dhcpv6 interface-id insert enable**

## Parameters

None

## Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

## 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 GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcpv6 interface-id insert enable
```

# 6.11.11 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**

## 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.<br>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.

**Precautions**

When the value of *packet-rate* is greater than 200, you need to run the **car packet-type dhcpv6-reply cir** *cir-value* command to increase the maximum rate of DHCPv6 Reply messages.

## 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
```

# 6.11.12 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.

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
```

# 6.11.13 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.
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
```

# 6.11.14 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 (.). |

## 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.

## Example

# Create an IPv6 address pool **DHCPv6POOL**.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 pool DHCPv6POOL
```

# 6.11.15 dhcpv6 relay advertise prefix-delegation route

## Function

The **dhcpv6 relay advertise prefix-delegation route** command enables a DHCPv6 relay agent to forward routing information of DHCPv6 prefix delegation (DHCPv6 PD) terminals.

The **undo dhcpv6 relay advertise prefix-delegation route** command disables a DHCPv6 relay agent from forwarding routing information of DHCPv6 PD terminals.

By default, a DHCPv6 relay agent does not forward routing information of DHCPv6 PD terminals.

## Format

**dhcpv6 relay advertise prefix-delegation route**

**undo dhcpv6 relay advertise prefix-delegation route**

## Parameters

None

## Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

The **dhcpv6 relay advertise prefix-delegation route** command is used on DHCPv6 relay agents. DHCPv6 PD terminals cannot advertise IPv6 routes. This command enables a DHCPv6 relay agent to add routes of DHCPv6 PD terminals to the routing table when DHCPv6 PD terminals apply for IP addresses from the DHCPv6 server through the DHCPv6 relay agent. The DHCPv6 relay agent then forwards the routing information to the DHCPv6 server.

**Prerequisites**

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**

This command takes effect only for the first-hop DHCPv6 relay agent connected to DHCPv6 PD terminals.

## Example

# Enable VLANIF10 to forward routing information of DHCPv6 PD terminals.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] ipv6
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] ipv6 enable
[HUAWEI-Vlanif10] dhcpv6 relay destination FC00::1:3
[HUAWEI-Vlanif10] dhcpv6 relay advertise prefix-delegation route
```

# 6.11.16 dhcpv6 relay prefix-delegation route

## Function

The **dhcpv6 relay prefix-delegation route** command saves routing information forwarded by a relay agent into a specified file.

The **undo dhcpv6 relay prefix-delegation route** command cancels the configuration.

By default, routing information forwarded by a relay agent into a specified file is not saved.

## Format

**dhcpv6 relay prefix-delegation route autosave** *file-name*

**undo dhcpv6 relay prefix-delegation route autosave**

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **autosave** | Backs up routing information learned from DHCPv6 PD terminals to the flash memory. | - |

| Parameter | Description | Value |
| --- | --- | --- |
| *file-name* | Specifies the path and file name of the file where routing information of DHCPv6 PD terminals is to be saved, for example, flash:/*.pdr. | The value is a string of 1 to 51 case-insensitive characters and is a combination of digits, letters, and characters. It cannot contain spaces.<br>**NOTE**<br>The file name cannot contain any less than sign (<), greater than sign (>), question mark (?), asterisk (*), comma (,), back quote (`), slash (/), backslash (\), single quotation mark ('), colon (:), or double quotation mark ("), and the left square bracket ([) and right square bracket (]) cannot exist in pairs. |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

The **dhcpv6 relay prefix-delegation route** command is used on DHCPv6 relay agents. This command saves routing information forwarded by a relay agent into a specified file.

After this command is run, the system immediately saves routing information, and then saves routing information again every two hours. The interval at which the system saves routing information cannot be set.

**Prerequisites**

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

## Example

# Save routing information forwarded by a relay agent into a specified file.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 relay prefix-delegation route autosave flash:/dhcpv6-pd.pdr
Info: The operation may take a few seconds, Please wait for a moment.done.
```

# 6.11.17 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* }

## 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. The specified interface can only be a Layer 2 interface. | - |

## Views

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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 run the **dhcpv6 relay destination** *ipv6-address* command to enable the DHCPv6 relay function on an interface.

When the client and the server are in the same VLAN, you can run the **dhcpv6 relay interface** *interface-type interface-number* command to specify the outbound interface of relay messages.

### Prerequisites

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

### Precautions

- When you run the **dhcpv6 relay interface** *interface-type interface-number* command in the VLANIF interface view to specify the outbound interface of relay messages, the specified interface can only be a Layer 2 interface. If the specified outbound interface is not in the VLAN corresponding to the VLANIF interface, add the interface to the VLAN.
- When both the **dhcpv6 relay destination** *ipv6-address* and **dhcpv6 relay interface** *interface-type interface-number* commands are configured, relay messages are preferentially sent to the configured IPv6 address based on routes.

## Example

# Enable the DHCPv6 relay function on VLANIF100 and set the destination address of relay messages to fc00:1::1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] dhcpv6 relay destination fc00:1::1
```

# 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] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] dhcpv6 relay destination fc00:1::1
```

# 6.11.18 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

VLANIF interface view, VBDIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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. The DHCP function has been enabled using the **dhcp enable** command in the system view.

2. A DHCPv6 server group has been created using the **dhcpv6 server group** command.
3. The IPv6 function has been enabled using the **ipv6 enable** 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 VLANIF100.

```
<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 vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] dhcpv6 relay server-select group1
```

# Configure the DHCPv6 server group named group 1 for the DHCPv6 relay agent on GE0/0/1.

```
<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 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] dhcpv6 relay server-select group1
```

# 6.11.19 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**

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *interface-type interface-number* | Specifies the interface type and number.<br>• *interface-type*: specifies the interface type. Currently, only loopback interfaces are supported.<br>• *interface-number*: specifies the interface number. | - |

## Views

System view, VBDIF interface view, VLANIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, MultiGE sub-interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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.

In addition, VBDIF interfaces functioning as gateways on distributed gateway devices use the same IPv6 address. If Layer 3 VXLAN gateways are distributed gateways and the IPv6 address is used to communicate with the server, the response packets from the server are forwarded to the incorrect distributed gateways (devices that do not send DHCPv6 request packets). To resolve this issue, you need to run the **dhcpv6 relay source-interface** *interface-type interface-number* command on each distributed gateway to specify the IPv6 address of the loopback interface as the source IPv6 address of the DHCPv6 relayed packets for ensuring that response packets from the server can be forwarded to the correct distributed gateways.

**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 **ipv6** command.
- A loopback interface has been created using the **interface loopback** *loopback-number* command.
- An IPv6 address has been configured for the loopback interface using the **ipv6 address** command.
- DHCP has been enabled globally using the **dhcp enable** command.
- In the interface view:
  - The IPv6 function has been enabled on the interface using the **ipv6 enable** 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.

If the DHCPv6 relay agent connects to the DHCPv6 server over a VPN network, you need to run the **ip binding vpn-instance** command to bind the loopback interface specified in the **dhcpv6 relay source-interface** command to the corresponding VPN instance.

## 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
```

# On GE0/0/1, 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 gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] dhcpv6 relay destination fc00:1::1
[HUAWEI-GigabitEthernet0/0/1] dhcpv6 relay source-interface loopback 5
```

# 6.11.20 dhcpv6 relay option79 insert enable

## 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, VBDIF interface view, VLANIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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**

- Before the **dhcpv6 relay option79 insert enable** command is configured, DHCP has been globally enabled using the **dhcp enable** command in the system view and IPv6 has been globally enabled using the **ipv6** command.
- Before the **dhcpv6 relay option79 insert enable** command is configured in the interface view, the DHCPv6 relay function has been enabled in the interface view.

**Precautions**

- 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 vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] dhcpv6 relay destination fc00:1::1
[HUAWEI-Vlanif100] dhcpv6 relay option79 insert enable
```

# 6.11.21 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**

## 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 GE0/0/1, and the client DUID is 0003000180FB063545B3, the Remote-ID option generated during the system parsing process is 0003000180FB063545B3 GigabitEthernet 0/0/1:0011.0022. | - |

| Parameter | Description | Value |
| --- | --- | --- |
| **user-defined** *text* | Specifies a user-defined format as the Remote-ID format. A user-defined format can be:<br>• 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.<br>For description of the keywords supported by the user-defined format, see **Table 6-77**.<br>• 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.<br>• 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. |

| 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 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 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 6-77** 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. |

| 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. |

**Prerequisites**

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

**Follow-up Procedure**

When the device functions as a DHCPv6 relay, you must run the **dhcpv6 remote-id insert enable** or **dhcpv6 remote-id rebuild 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 \.
- 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"
```

# 6.11.22 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

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk 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, 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**

DHCP has been enabled globally using the **dhcp enable** 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
```

# 6.11.23 dhcpv6 remote-id rebuild enable

## Function

Using the **dhcpv6 remote-id rebuild enable** command, you can enable the function of appending the remote ID to DHCPv6 relay messages.

Using the **undo dhcpv6 remote-id rebuild 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 rebuild enable**

**undo dhcpv6 remote-id rebuild enable**

## Parameters

None

## Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

## Default Level

2: Configuration level

## Usage Guidelines

The remote ID carries information about a client and identifies a client. The DHCPv6 server can make decisions about address allocation, parameter setting, prefix agent according to the remote ID. The format of the remote ID is defined by the vendor. Usually, the remote ID carries the phone number and user name in a dial-up connection, or the peer IP address and access interface in a point-to-point connection.

Before running the **dhcpv6 remote-id rebuild enable** command, you must run the **dhcp enable** command to enable DHCP globally.

## Example

# Enable the function of appending the remote ID to DHCPv6 relay messages on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcpv6 remote-id rebuild enable
```

# 6.11.24 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** } *

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **allow-hint** | Specifies the DHCPv6 server to allocate addresses, prefixes, and prefix lengths based on the DHCPv6 client requests.<br>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.<br>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. | - |

## 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 **link-address** command or **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.
  - When the DHCPv6 server is enabled in the system view, the DHCPv6 server cannot assign network parameters (such as IPv6 addresses, DNS, NIS, and SNTP servers) to clients if no relay exists. To enable the DHCPv6

server to assign network parameters, enable the DHCPv6 server function in the interface view.

- 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 **dhcpv6 server** 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
```

# 6.11.25 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**

## 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 case-sensitive characters without spaces. The value can contain digits, letters, underscores (_), and periods (.). |
| **allow-hint** | Specifies the DHCPv6 server to allocate addresses, prefixes, and prefix lengths based on the DHCPv6 client requests.<br>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 IPv6 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.<br>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. | - |

| Parameter | Description | Value |
| --- | --- | --- |
| **unicast** | Specifies the unicast communication between the DHCPv6 client and DHCPv6 server during IPv6 address lease. | - |

## Views

VLANIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-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 VLANIF100 and set the priority of pool1 to 255.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
```

```
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] dhcpv6 server pool1 preference 255
```

# Associate DHCPv6 address pool pool1 with GE0/0/1 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] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] dhcpv6 server pool1 preference 255
```

# 6.11.26 dhcpv6-server (DHCPv6 server group view)

## 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* [ **interface** *interface-type interface-number* ]

**undo dhcpv6-server** *ipv6-address* [ **interface** *interface-type interface-number* ]

## 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. |
| **interface** *interface-type interface-number* | Specifies the type and number of an outbound interface for DHCPv6 packets.<br>• *interface-type* specifies the type of an interface.<br>• *interface-number* specifies the number of an interface. | - |

## 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 of the remote DHCPv6 server or the next-hop relay agent on the next-hop relay agent.

**Prerequisites**

1. The DHCP function has been enabled using the **dhcp enable** command in the system view.
2. A DHCPv6 server group has been created using the **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
```

# 6.11.27 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. |
| **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
```

# 6.11.28 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.

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. 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

**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.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 server group DHCPv6-srv1
[HUAWEI-dhcpv6-server-group-DHCPv6-srv1]
```

# 6.11.29 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 mode.
Stateful DHCPv6 client is in BOUND state.
Preferred server DUID   : 000300060819A6CDA894
  Reachable via address : FE80::A19:A6FF:FECD:A897
IA NA IA ID 0x00000051 T1 43200 T2 69120
  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
```

**Table 6-78** Description of the display dhcpv6 client command output

| Item | Description |
| --- | --- |
| Vlanif10 is in stateful DHCPv6 client mode. | The VLANIF10 interface is in stateful DHCPv6 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. |
| 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. |
| Lifetime valid 120 seconds, preferred 60 seconds | The valid lifetime is 120 seconds and preferred lifetime is 60 seconds. |
| 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. |

# 6.11.30 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.

## 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 6-79** Description of the **display dhcpv6 client prefix** command output

| Item | Description |
| --- | --- |
| Prefix name | IPv6 address prefix name. |
| Prefix | IPv6 address prefix. |

| Item | Description |
| --- | --- |
| Life time(sec) | • valid: Period during which an IPv6 address prefix is valid.<br>• preferred: Period during which an IPv6 address prefix is valid since its lease is renewed. |

# 6.11.31 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

## Default Level

1: Monitoring level

## Usage Guidelines

When the device functions as a DHCPv6 client, you can run this command to view DHCPv6 message statistics.

## Example

# Display DHCPv6 message statistics on the DHCPv6 client.

```
<HUAWEI> display dhcpv6 client statistics
 Message statistics of interface Vlanif10:
   Message                 Received
   Advertise               1
   Reply                   1
   Reconfigure             0
   Invalid                 0
```

```
Dropped untrusted reply  0

Message                   Sent
Solicit                 1
Request                   1
Confirm                   0
Renew                     0
Rebind                    0
Release                   0
Decline                   0
Information-request       0
```

**Table 6-80** 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. |
| Dropped untrusted reply | When the **dhcp snooping check local-reply enable** command is configured on a device that functions as a DHCP client, the **dhcp snooping trusted** command must be configured on the interface connected to the DHCP server. Otherwise, the DHCP client discards response messages from the DHCP server. |
| 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. |
| Renew | Number of Renew messages sent by the DHCPv6 client. |
| Rebind | Number of Rebind messages sent by the DHCPv6 client. |

| Item | Description |
| --- | --- |
| 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. |

# 6.11.32 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.

```
<HUAWEI> display dhcpv6 duid
The device's DHCPv6 unique identifier: 0001000117C667C280FB063545B3
```

# 6.11.33 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
```

**Table 6-81** 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.<br>To configure this item, run the **dhcpv6 relay source-interface** command. |
| Option79 insert | Whether to insert the Option79 field into DHCPv6 messages. The value can be:<br>• enable: The Option79 field is inserted into DHCPv6 messages.<br>• disable: The Option79 field is not inserted into DHCPv6 messages.<br>To configure this item, run the **dhcpv6 relay option79 insert enable** command. |

# 6.11.34 display dhcpv6 relay prefix-delegation

## Function

Using the **display dhcpv6 relay prefix-delegation** command, you can view DHCPv6 PD routing information forwarded by the DHCPv6 Relay.

## Format

**display dhcpv6 relay prefix-delegation** { **client** [ **interface** *interface-type interface-number* ] | **route** [ **interface** *interface-type interface-number* ] }

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **client** | Displays information about DHCPv6 PD clients. | - |
| **interface** *interface-type interface-number* | Specifies the type and the number of an interface. | - |

| Parameter | Description | Value |
| --- | --- | --- |
| **route** | Displays routing information learned from DHCPv6 PD clients. | - |

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

The **display dhcpv6 relay prefix-delegation** command is used on DHCPv6 relay agents. This command displays routing information that DHCPv6 relay agents learn from DHCPv6 PD terminals, including the destination IPv6 address, next hop address, outbound interface, and protocol type of each route. You can also use this command to view DHCPv6 PD routing information forwarded by the DHCPv6 Relay.

## Example

# Display DHCPv6 PD routing information forwarded by the DHCPv6 Relay.

```
<HUAWEI> display dhcpv6 relay prefix-delegation route
------------------------------------------------------------------------------
 Destination   : FC00:1::/96
 Next-hop      : FC00:2::1
 Interface     : Vlanif62
 Protocol type : Unr
 Destination   : FC00:2::/96
 Next-hop      : FC00:2::2
 Interface     : Vlanif62
 Protocol type : Unr
------------------------------------------------------------------------------
 Total count : 1  Print count : 1
```

**Table 6-82** Description of the display dhcpv6 relay prefix-delegation route command output

| Item | Description |
| --- | --- |
| Destination | Destination network segment of a route. |
| Next-hop | Next hop address of a route. |
| Interface | Outbound interface of a route. |
| Protocol type | Protocol type used by a route. |
| Total count | Number of routes displayed. |

| Item | Description |
| --- | --- |
| Print count | Number of routes printed. A maximum of 512 routes can be printed. |

# Display information about DHCPv6 PD terminals.

```
<HUAWEI> display dhcpv6 relay prefix-delegation client
------------------------------------------------------------------------------
 DUID_EN       : 000612E978E600E04C774E5A
 Interface     : Vlanif62
 IPv6 address  : FC00:1::4E5A
    IA PD      : IA ID 1, T1 600, T2 900,
       IA Prefix: FC00:3::/96
          preferred lifetime 900 , valid lifetime 1200
          expired at 2010.02.21 15:01:54
       IA Prefix: FC00:4::/96
          preferred lifetime 900 , valid lifetime 1200
          expired at 2010.02.21 15:01:54
------------------------------------------------------------------------------
 Total count : 1  Print count : 1
```

**Table 6-83** Description of the display dhcpv6 relay prefix-delegation client command output

| Item | Description |
| --- | --- |
| DUID_EN | DHCPv6 unique identifier (DUID) of a client, which is defined by the vendor. |
| Interface | Interface to which a client is connected. |
| IPv6 address | IPv6 address of a client. |
| IA PD | IPv6 prefix contained in the packet sent from a client. |
| Total count | Number of client records displayed. |
| Print count | Number of client records printed. A maximum of 512 records can be printed. |

# 6.11.35 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* ]

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **interface** *interface-type interface-number* | Specifies the type and number of an interface.<br>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
```

**Table 6-84** 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. |

# 6.11.36 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. |
| **conflict address** | Specifies the conflicted IPv6 addresses in the IPv6 address pool. | - |

| Parameter | Description | Value |
| --- | --- | --- |
| *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: example.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
  conflict-address expire-time: 61
  renew-time-percent : 55
  rebind-time-percent : 85
  Active normal clients: 0
  Active pd clients: 0    Logging : Enable
```

**Table 6-85** 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.<br>You can set the prefix using the **address prefix** command. |
| Prefix delegation | Agent prefix bound to the IPv6 address pool.<br>You can set the agent prefix using the **prefix-delegation** command. |
| Information refresh time | Time for updating configuration parameters assigned to clients through stateless DHCPv6 address autoconfiguration.<br>You can set the time using the **information-refresh** command. |
| DNS server address | DNS server address configured for the IPv6 address pool.<br>You can configure the DNS server address using the **dns-server** command. |
| SIP server address | SIP server address configured for the IPv6 address pool.<br>You can configure the SIP server address using the **sip-server** command. |
| NIS server address | NIS server address configured for the IPv6 address pool.<br>You can configure the NIS server address using the **nis-server** command. |
| NISP server address | NISP server address configured for the IPv6 address pool.<br>You can configure the NISP server address using the **nisp-server** command. |
| SNTP server address | SNTP server address configured for the IPv6 address pool.<br>You can configure the SNTP server address using the **sntp-server** command. |

| Item | Description |
| --- | --- |
| Domain name | Domain name suffix allocated by the DHCPv6 server to the client.<br>You can configure the domain name suffix using the **dns-domain-name** command. |
| SIP server domain name | SIP domain name suffix allocated by the DHCPv6 server to the client.<br>You can configure the SIP domain name suffix using the **sip-domain-name** command. |
| NIS server domain name | NIS domain name suffix allocated by the DHCPv6 server to the client.<br>You can configure the NIS domain name suffix using the **nis-domain-name** command. |
| NISP server domain name | NISP domain name suffix allocated by the DHCPv6 server to the client.<br>You can configure the NISP domain name suffix using the **nisp-domain-name** command. |
| Vendor-specific option | Vendor-defined options.<br>You can configure the vendor-defined options using the **vendor-specific** and **suboption** commands. |
| conflict-address expire-time | Aging time of conflicted addresses.<br>You can set the aging time using the **conflict-address expire-time** command. |
| renew-time-percent | The percentage of the lease renewal time in the preferred lifetime.<br>You can set the percentage of the lease renewal time in the preferred lifetime using the **renew-time-percent rebind-time-percent** command. |
| rebind-time-percent | The percentage of the lease rebinding time in the preferred lifetime.<br>You can set the percentage of the lease rebinding time in the preferred lifetime using the **renew-time-percent rebind-time-percent** command. |

| Item | Description |
| --- | --- |
| Active normal clients | Number of DHCP clients. |
| Active pd clients | Number of DHCPv6 PD clients. |
| Logging | Whether the function of recording a log when the DHCPv6 or DHCPv6 PD server allocates an IPv6 address or prefix is enabled. The value can be:<br>• Enable: The function is enabled.<br>• Disable: The function is disabled.<br>To configure this item, run the **logging** command. |

# 6.11.37 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.<br>• *interface-type* specifies the interface type.<br>• *interface-number* specifies the interface number. | - |

## Views

All views

## Default Level

1: Monitoring level

## 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
------------------------------------------------------------------------------
GigabitEthernet0/0/1   Relay         FC00:4::3
Vlanif10               Relay         FC00:1::1:1
------------------------------------------------------------------------------
 Print count : 2                     Total count : 2
```

**Table 6-86** 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.<br>Address pointing to the DHCPv6 server, address of the next-hop DHCPv6 relay, or DHCPv6 server group.<br>To configure the address, run the **dhcpv6 relay destination** or **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. |

# 6.11.38 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* ] ]

## 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 6-87** 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.<br>You can configure the IPv6 pool name using the **dhcpv6 server** command. |

# 6.11.39 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.<br>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.

```
<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 6-88** Description of the display dhcpv6 server group command output

| Item | Description |
| --- | --- |
| DHCPv6 Group-name | Name of a DHCPv6 server group.<br>To set this parameter, run the **dhcpv6 server group** command. |
| server-ip | IPv6 address of a DHCPv6 server in a DHCPv6 server group.<br>To set this parameter, run the **dhcpv6-server (DHCPv6 server group view)** command. |

# 6.11.40 display dhcpv6 statistics

## Function

The **display dhcpv6 statistics** command displays DHCPv6 packet statistics.

## Format

**display dhcpv6 statistics** [ **verbose** ]

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **verbose** | Displays statistics about socket packet sending failures. | - |

## 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

# Display 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 6-89** 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. |

| Item | Description |
| --- | --- |
| Advertise | Number of ADVERTISE packets received by the device. |
| 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. |

| Item | Description |
| --- | --- |
| Max-user limit or Add bindtable failed | Information displayed if the DHCPv6 service is abnormal. The displayed information includes:<br>• Max-user limit: Total number of DHCPv6 messages discarded because the maximum number of users (configured by running the **dhcp snooping max-user-number** command) is exceeded.<br>• Add bindtable failed: Total number of DHCPv6 packets discarded because dynamic binding entries are added. New dynamic binding entries may be added if the user-side interface is Down, or IPSG is configured but ACL resources are insufficient.<br>• High cpu occupancy: Total number of DHCPv6 packets discarded because the CPU usage is excessively high.<br>• Port blocked: Total number of DHCPv6 packets discarded because the inbound interface is blocked.<br>• Rx buffers full: Total number of DHCPv6 packets discarded because the remaining queue length is shorter than the reserved threshold.<br>• L2fdb lookup failed: Total number of DHCPv6 Reply packets discarded because the DHCP snooping module fails to find user-side interfaces.<br>• Bad vlan id: Total number of DHCPv6 packets discarded because the interfaces receiving the DHCPv6 packets are not added to the VLANs corresponding to the VLAN tags carried in the packets or the DHCPv6 packets received on interfaces carry VLAN tags not in the range from 1 to 4094.<br>• Memory exhausted: Total number of DHCPv6 packets discarded because the memory is exhausted.<br>• L3if protocol down: Total number of DHCPv6 packets discarded because |

| Item | Description |
| --- | --- |
| | the Layer 3 protocol of the source interface goes Down.<br>• Rate limit: Total number of DHCPv6 packets discarded because rates of the messages exceed the limit, when the **dhcpv6 packet-rate** or **dhcp snooping check dhcpv6-rate enable** command is configured.<br>• Bad packet length: Total number of DHCPv6 packets discarded because the packet length is not in the range of 50 to 2048 bytes.<br>• Bad ip header checksum: Total number of DHCPv6 packets discarded because the checksum of the IP header is incorrect.<br>• Bad request: Total number of invalid DHCPv6 request packets that are discarded, when the **dhcp snooping check dhcp-request enable** or **dhcp snooping check dhcpv6-request mac** command is configured to check the validity of DHCPv6 request packets.<br>• Bad reply: Total number of DHCPv6 response packets discarded by untrusted interfaces configured with the **dhcp snooping enable** command.<br>• Client transferred: Total number of DHCPv6 packets discarded because the **undo dhcp snooping user-transfer enable** command is configured to disable interface flapping.<br>• Other error: Total number of DHCPv6 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. |

## 6.11.41 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.

## 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. It can be the combination of letters, digits, underscores (_), hyphens (-), or dots (.) and cannot be set to only hyphens (-) or hyphens (--). |

## 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 **example.com** for the address pool **pool1**.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 pool pool1
[HUAWEI-dhcpv6-pool-pool1] dns-domain-name example.com
```

# 6.11.42 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.

## 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
```

# 6.11.43 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** *start-ipv6-address* [ **to** *end-ipv6-address* ]

**undo excluded-address** *start-ipv6-address* [ **to** *end-ipv6-address* ]

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *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. |

| 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.<br>*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.

- 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
```

# 6.11.44 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

## 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
```

# 6.11.45 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**

## 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

VLANIF interface view, Eth-Trunk interface view, GE interface view, XGE interface view, MultiGE interface view, MultiGE sub-interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk sub-interface view, GE sub-interface view, XGE sub-interface view, 25GE sub-interface view, 40GE sub-interface view, 100GE sub-interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

After you run the **ipv6 address auto dhcp** [ **rapid-commit** ] command on 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 **ipv6** command in the system view.
2. IPv6 functions have been enabled on interfaces using the **ipv6 enable** 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 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 VLANIF100 to obtain IPv6 addresses and other configuration parameters from the DHCPv6 server using DHCPv6 stateful address autoconfiguration.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ipv6 enable
[HUAWEI-Vlanif100] ipv6 address auto link-local
[HUAWEI-Vlanif100] ipv6 address auto dhcp
```

# Configure the interface GE0/0/1 to obtain IPv6 addresses and other configuration parameters from the DHCPv6 server using DHCPv6 stateful address autoconfiguration.

```
<HUAWEI> system-view
[HUAWEI] ipv6
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipv6 enable
[HUAWEI-GigabitEthernet0/0/1] ipv6 address auto link-local
[HUAWEI-GigabitEthernet0/0/1] ipv6 address auto dhcp
```

# 6.11.46 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.<br>*ipv6-prefix-length*: The value is an integer that ranges from 16 to 128. |

## 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 **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 **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.
  - When the DHCPv6 server is enabled in the system view, the DHCPv6 server cannot assign network parameters (such as IPv6 addresses, DNS, NIS, and SNTP servers) to clients if no relay exists. To enable the DHCPv6 server to assign network parameters, enable the DHCPv6 server function in the interface view.
- 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 **dhcpv6 server** 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).

## 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
```

# 6.11.47 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.

## Example

# Lock the address pool **global1**.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 pool global1
[HUAWEI-dhcpv6-pool-global1] lock
```

# 6.11.48 logging (IPv6 address pool view)

## Function

The **logging** command enables the function of recording a log when the DHCPv6 or DHCPv6 PD server allocates an IPv6 address or prefix in the IPv6 address pool view.

The **undo logging** command disables the function of recording a log when the DHCPv6 or DHCPv6 PD server allocates an IPv6 address or prefix in the IPv6 address pool view.

By default, this function is disabled.

## Format

**logging** [ **allocation-address-success** | **allocation-prefix-success** | **detect-address-conflict** | **release-address-success** | **release-prefix-success** | **renew-address-success** | **renew-prefix-success** ] *

**undo logging** [ **allocation-address-success** | **allocation-prefix-success** | **detect-address-conflict** | **release-address-success** | **release-prefix-success** | **renew-address-success** | **renew-prefix-success** ] *

## Parameters

NOTE

If the following parameters are not specified, the function of recording related logs is enabled or disabled.

| Parameter | Description | Value |
| --- | --- | --- |
| **allocation-address-success** | Displays a log when an IPv6 address is successfully allocated. | - |
| **allocation-prefix-success** | Displays a log when an IPv6 prefix is successfully allocated. | - |
| **detect-address-conflict** | Displays a log when an IPv6 address conflict is detected. | - |
| **release-address-success** | Displays a log when an IPv6 address is released. | - |
| **release-prefix-success** | Displays a log when an IPv6 prefix is released. | - |
| **renew-address-success** | Displays a log when an IPv6 address is renewed. | - |
| **renew-prefix-success** | Displays a log when an IPv6 prefix is renewed. | - |

## Views

IPv6 address pool view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

This command is applied to the DHCPv6 or DHCPv6 PD server. After the **logging** command is configured, the server records a log if an IPv6 address or prefix is allocated, renewed, or released, or an IPv6 address or prefix conflict is detected, facilitating routine maintenance and fault locating.

You can run the **display dhcpv6 pool** command to check the status of the log recording function on the server.

**Prerequisites**

An IPv6 address pool has been created using the **dhcpv6 pool** command.

**Precautions**

- After the log recording function is enabled, the server may frequently record logs if a large number of clients request for IPv6 addresses or prefixes, deteriorating device performance.
- 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 in the *CLI-based Configuration - Device Management Configuration Guide*.

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 function of recording a log when the server allocates an IPv6 address or prefix in the IPv6 address pool **pool1**.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 pool pool1
[HUAWEI-dhcpv6-pool-pool1] logging
```

# 6.11.49 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. It can be the combination of letters, digits, underscores (_), hyphens (-), or dots (.) and cannot be set to a single hyphen (-) or consecutive hyphens (--). |

## Views

IPv6 address pool view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

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
```

# 6.11.50 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. It can be the combination of letters, digits, underscores (_), hyphens (-), or dots (.) and cannot be set to only hyphens (-) or hyphens (--). |

## 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
```

# 6.11.51 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*

## 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
```

# 6.11.52 nis-server

## Function

The **nis-server** command configures the NIS server address assigned to the DHCPv6 client for the IPv6 address pool.

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
```

# 6.11.53 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.<br>The IPv6 address prefix length ranges from 1 to 128. |

| Parameter | Description | Value |
| --- | --- | --- |
| *assign-prefix-length* | Specifies the default prefix length.<br>**NOTE**<br>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.<br>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.<br>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.<br>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.<br>When the preferred lifetime is set to infinite, the valid lifetime must be set to infinite. | - |

| 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.<br>• *hours*: indicates hours. The value is an integer that ranges from 0 to 23.<br>• *minutes*: indicates minutes. The value is an integer that ranges from 0 to 59.<br>• *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.<br>• *hours*: indicates hours. The value is an integer that ranges from 0 to 23.<br>• *minutes*: indicates minutes. The value is an integer that ranges from 0 to 59.<br>• *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

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
```

# 6.11.54 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.

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.<br>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.

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
```

# 6.11.55 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* ]

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **interface** *interface-type interface-number* | Clears DHCPv6 message statistics on a specified interface.<br>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
```

# 6.11.56 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* ]

## 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.<br>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.

**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
```

# 6.11.57 reset dhcpv6 relay prefix-delegation route

## Function

The **reset dhcpv6 relay prefix-delegation route** command deletes routing information learned from DHCPv6 PD terminals on a DHCPv6 relay agent.

## Format

**reset dhcpv6 relay prefix-delegation route** [ **vpn6-instance** *vpn-instance-name* ] *ipv6-address mask-length*

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *ipv6-address* | Specifies the destination IPv6 address of the routes to be deleted. | 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. |

| Parameter | Description | Value |
| --- | --- | --- |
| *mask-length* | Specifies the mask length of the IPv6 address. | The value is an integer ranging from 0 to 128 |
| **vpn6-instance** *vpn-instance-name* | Specifies the VPN instance name. | The value must be an existing VPN instance name. |

## Views

User view

## Default Level

3: Management level

## Usage Guidelines

The **reset dhcpv6 relay prefix-delegation route** command is used on DHCPv6 relay agents. Before collecting routing information about a specified IPv6 address, run the **reset dhcpv6 relay prefix-delegation route** command to delete the existing routing information.

## Example

# Delete routing information with destination IPv6 address fc00:1::1 learned from DHCPv6 PD terminals.

```
<HUAWEI> reset dhcpv6 relay prefix-delegation route fc00:1::1 64
```

# 6.11.58 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.<br>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

## 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
```

# 6.11.59 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 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
```

# 6.11.60 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
```

# 6.11.61 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. It can be the combination of letters, digits, underscores (_), hyphens (-), or dots (.) and cannot be set to a single hyphen (-) or consecutive hyphens (--). |

## 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**

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
```

# 6.11.62 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**

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
```

# 6.11.63 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. |

## 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
```

# 6.11.64 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** *ipv6-address* **duid** *client-duid* [ **iaid** *iaid* ] [ **life-time** { *valid-lifetime* | **infinite** } { *preferred-lifetime* | **infinite** } ]

**undo static-bind address** *ipv6-address*

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *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. |

| Parameter | Description | Value |
| --- | --- | --- |
| **infinite** | Sets the lifetime of the bound entries to infinite. | - |

## Views

IPv6 address pool view

## Default Level

2: Configuration level

## 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
```

# 6.11.65 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*

## 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.<br>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.<br>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**

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
```

# 6.11.66 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*

## 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. |
| **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.

## 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
```

# 6.11.67 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

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.

## 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
```

# 6.12 IPv6 DNS Configuration Commands

## 6.12.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

## 6.12.2 display dns ipv6 dynamic-host

### Function

The **display dns ipv6 dynamic-host** command displays IPv6 dynamic DNS entries.

### Format

**display dns ipv6 dynamic-host** [ **vpn-instance** *vpn-instance-name* | **all** ]

### Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **vpn-instance** *vpn-instance-name* | Displays IPv6 dynamic DNS entries of a specified VPN instance. | The value must be an existing VPN instance name. |
| **all** | Displays all IPv6 dynamic DNS entries, including both public and private DNS entries.<br>**NOTE**<br>If neither **vpn-instance** *vpn-instance-name* nor **all** is specified, only public IPv6 dynamic DNS entries are displayed. | - |

## Views

All views

## Default Level

1: Monitoring level

## Usage Guidelines

You can run the **display dns ipv6 dynamic-host** command to view IPv6 dynamic DNS entries and check whether domain names match the mapping entries.

## Example

# Display IPv6 dynamic DNS entries.

```
<HUAWEI> display dns ipv6 dynamic-host
No  Domain-name       Ipv6Address     TTL
1   example           FC00:1::1       6
```

# Display IPv6 dynamic DNS entries of the VPN instance vpn1.

```
<HUAWEI> display dns ipv6 dynamic-host vpn-instance vpn1
No      Domain-name                     Ipv6Address          TTL          VPN-Instance
1       example                         2001:db8::2          6            vpn1
```

**Table 6-90** Description of the **display dns ipv6 dynamic-host** command output

| Item | Description |
| --- | --- |
| No | Sequence number of a dynamic IPv6 DNS entry. |
| Domain-name | Domain name. |
| Ipv6Address | IPv6 address mapping the domain name. |
| TTL | TTL value of the dynamic domain names in the cache (in seconds). |
| VPN-Instance | VPN instance name. |

# 6.12.3 display ipv6 host

## Function

The **display ipv6 host** command displays the IPv6 static DNS entries.

## Format

**display ipv6 host** [ **vpn-instance** *vpn-instance-name* | **all** ]

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **vpn-instance** *vpn-instance-name* | Displays IPv6 static DNS entries of a specified VPN instance. | The value must be an existing VPN instance name. |
| **all** | Displays all IPv6 static DNS entries, including both public and private static DNS entries.<br>**NOTE**<br>If neither **vpn-instance** *vpn-instance-name* nor **all** is specified, only public IPv6 static DNS entries are displayed. | - |

## 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 IPv6 static DNS entries.

```
<HUAWEI> display ipv6 host
Host                 Age       Flags           IPv6Address(es)
www.example.com      0         static          FC00:1::8
www.sohu.com         0         static          FC00:1::9
```

# Display IPv6 static DNS entries of the VPN instance vpn1.

```
<HUAWEI> display ipv6 host vpn-instance vpn1
Host          Age        Flags       IPv6Address(es)         VPN-Instance
RTB           0          static      2001:db8::1             vpn1
```

**Table 6-91** Description of the **display ipv6 host** command output

| Item | Description |
| --- | --- |
| Host | Host name.<br>The value is set using the **ipv6 host** command. |

| Item | Description |
| --- | --- |
| Age | Aging time. The value 0 indicates that the entry is not aged out. |
| Flags | Identifiers. The value static indicates a static domain name. |
| IPv6Address(es) | IPv6 address mapping the domain name.<br>The value is set using the **ipv6 host** command. |
| VPN-Instance | VPN instance name.<br>The value is set using the **ipv6 host** command. |

## 6.12.4 dns server ipv6

### Function

The **dns server ipv6** command configures the IPv6 address of a DNS server.

The **undo dns server ipv6** command deletes the IPv6 address of a DNS server.

By default, no IPv6 addresses of DNS servers are configured.

### Format

**dns server ipv6** *ipv6-address* [ *interface-type interface-number* ] [ **vpn-instance** *vpn-instance-name* ]

**undo dns server ipv6** *ipv6-address* [ *interface-type interface-number* ] [ **vpn-instance** *vpn-instance-name* ]

### 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. |

| Parameter | Description | Value |
| --- | --- | --- |
| *interface-type interface-number* | Specifies the type and number of an outbound interface that communicates with the DNS server. | - |
| **vpn-instance** *vpn-instance-name* | Specifies the name of a VPN instance. | The value must be an existing VPN instance name. |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

The 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 IPv6 address of the DNS server. The DNS client sends requests to the specified DNS server for domain name resolution.

During dynamic domain name resolution, the switch sends a domain name resolution request to the DNS servers according to the order in which they were configured. If the domain name resolution request on the first DNS server times out, the device sends the request to the next DNS server.

**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.

A maximum of six DNS server IP (IPv4 and IPv6) addresses can be configured on the switch.

If **vpn-instance** *vpn-instance-name* is specified, the system sends domain name resolution requests only to the DNS servers bound to the specified VPN instance.

## Example

# Configure the IPv6 address of the DNS server to fc00:1::1.

```
<HUAWEI> system-view
[HUAWEI] dns server ipv6 fc00:1::1
```

# 6.12.5 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 DNS server.

The **undo dns server ipv6 source-ip** command deletes the source IPv6 address used for the local end functioning as the DNS client to communicate with the DNS server.

By default, no source IPv6 address is configured for the local end functioning as the DNS client to communicate with the DNS server.

## Format

**dns server ipv6 source-ip** *ipv6-address* [ **vpn-instance** *vpn-instance-name* ]

**undo dns server ipv6 source-ip** [ **vpn-instance** *vpn-instance-name* ]

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *ipv6-address* | Specifies the source IPv6 address for the local end functioning as the DNS client to communicate with the 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. |
| **vpn-instance** *vpn-instance-name* | Specifies the name of a VPN instance. | The value must be an existing VPN instance name. |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

### Usage Scenario

After the source IPv6 address is specified, the DNS client uses the specified IPv6 address to communicate with the DNS server. This ensures communication

security. If no source IPv6 address is specified, the DNS client needs to select a source IPv6 address according to the destination address each time it sends an IPv6 DNS request.

**Precautions**

If only one route from the DNS server to the client with an IPv6 address is reachable, you need to specify the source IPv6 address in the DNS query message when the DNS client sends a DNS query to the server.

If **vpn-instance** *vpn-instance-name* is specified, the specified source IPv6 address is used only when the device communicates with the DNS server bound to the specified VPN instance.

## Example

# Configure the source IPv6 address that the DNS client uses to communicate with the DNS server to fc00:1::1.

```
<HUAWEI> system-view
[HUAWEI] dns server ipv6 source-ip fc00:1::1
```

# 6.12.6 ipv6 host

## Function

The **ipv6 host** command configures an IPv6 static DNS entry.

The **undo ipv6 host** command deletes an IPv6 static DNS entry.

By default, no IPv6 static DNS entry is configured.

## Format

**ipv6 host** *host-name ipv6-address* [ **vpn-instance** *vpn-instance-name* ]

**undo ipv6 host** *host-name* [ *ipv6-address* [ **vpn-instance** *vpn-instance-name* ] ]

## 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 (_). |

| Parameter | Description | Value |
| --- | --- | --- |
| *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. |
| **vpn-instance** *vpn-instance-name* | Specifies the name of a VPN instance. | The value must be an existing VPN instance name. |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

When requesting the IPv6 address mapping a domain name, the DNS client searches for the specified domain name in the static DNS table to obtain the corresponding IPv6 address. The **ipv6 host** command configures an IPv6 static DNS entry.

**Precautions**

Each domain name supports a maximum of eight IPv6 addresses.

## Example

# Configures an IPv6 static DNS entry mapping the host named **www.example.com**.

```
<HUAWEI> system-view
[HUAWEI] ipv6 host www.example.com fc00:1::8
```

# 6.12.7 reset dns ipv6 dynamic-host

## Function

The **reset dns ipv6 dynamic-host** command clears IPv6 dynamic DNS entries.

## Format

**reset dns ipv6 dynamic-host** [ **vpn-instance** *vpn-instance-name* | **all** ]

### Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **vpn-instance** *vpn-instance-name* | Clears IPv6 dynamic DNS entries of a specified VPN instance. | The value must be an existing VPN instance name. |
| **all** | Clears all IPv6 dynamic DNS entries, including both public and private DNS entries.<br>**NOTE**<br>If neither **vpn-instance** *vpn-instance-name* nor **all** is specified, only public IPv6 dynamic DNS entries are cleared. | - |

### Views

User view

### Default Level

2: Configuration level

### Usage Guidelines

**Usage Scenario**

After confirming the action of deleting IPv6 dynamic DNS entries, you can run the **reset dns ipv6 dynamic-host** command to delete them.

**Precautions**

IPv6 dynamic DNS entries cannot be restored after being deleted. Confirm the action before you run the command.

### Example

# Clear all IPv6 dynamic DNS entries.

```
<HUAWEI> reset dns ipv6 dynamic-host all
```

# 6.13 IPv6 over IPv4 Tunnel Configuration Commands

## 6.13.1 Command Support

Only the following switch models support the IPv6 over IPv4 Tunnel:

S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S

# 6.13.2 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, 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 IPv4 address is in dotted decimal notation.<br>The IPv6 address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. |

## Views

Tunnel interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

When configuring a GRE, MPLS TE, IPv4 over IPv6 tunnel or 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.

**Prerequisites**

A tunnel interface has been created using the **interface tunnel** command, and the encapsulation mode is set to GRE, MPLS TE, 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.

You can configure a main interface working in Layer 3 mode as the source tunnel interface.

On the GRE, MPLS TE, IPv4 over IPv6 tunnel or manual IPv6 over IPv4 tunnel, the destination address of the local tunnel interface is the source address of the remote tunnel interface, and the source address of the local tunnel interface is the destination address of the remote tunnel interface.

## Example

# Establish a manual IPv6 over IPv4 tunnel between VLANIF 10 at 10.1.1.1 on switch HUAWEI1 and VLANIF 20 at 10.2.1.1 on switch HUAWEI2.

```
<HUAWEI1> system-view
[HUAWEI1] interface tunnel 1
[HUAWEI1-Tunnel1] tunnel-protocol ipv6-ipv4
[HUAWEI1-Tunnel1] source 10.1.1.1
[HUAWEI1-Tunnel1] destination 10.2.1.1
<HUAWEI2> system-view
[HUAWEI2] interface tunnel 1
[HUAWEI2-Tunnel1] tunnel-protocol ipv6-ipv4
[HUAWEI2-Tunnel1] source 10.2.1.1
[HUAWEI2-Tunnel1] destination 10.1.1.1
```

# Set the destination address of the GRE tunnel Tunnel1 to 10.1.1.1 that belongs to vpn1.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vpn1
[HUAWEI-vpn-instance-vpn1] ipv4-family
[HUAWEI-vpn-instance-vpn1-af-ipv4] route-distinguisher 100:1
[HUAWEI-vpn-instance-vpn1-af-ipv4] quit
[HUAWEI-vpn-instance-vpn1] quit
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol gre
[HUAWEI-Tunnel1] destination vpn-instance vpn1 10.1.1.1
```

# 6.13.3 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*

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *interface-number* | Specifies the number of the tunnel interface. | The value is an integer that ranges from 0 to 2047 . |

## Views

System view

## Default Level

2: Configuration level

## Usage Guidelines

### Usage Scenario

To forward data over a tunnel, ensure that the tunnel has been created. The system supports the following types of tunnels:

- LSP (Static LSP, BGP LSP, LDP LSP)
- MPLS TE
- 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

Tunnel interface numbers are valid on the local device only. You can configure different numbers for the tunnel interfaces on the two ends.

### Follow-up Procedure

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. Then basic configurations are performed based on the encapsulation protocol:

- On an MPLS TE tunnel, run the **destination**, **mpls te tunnel-id**, **mpls te signal-protocol**, and **mpls te commit** commands.
- On the GRE, IPv4 over IPv6 tunnel or manual IPv6 over IPv4 tunnel, run the **source** and **destination** commands.

## Example

# Create a tunnel interface.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1]
```

# 6.13.4 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** { *source-ip-address* | *interface-type interface-number* }

**undo source**

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *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.<br>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. The following types of interfaces are often used: VLANIF and loopback. | - |

## Views

Tunnel interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

When configuring a GRE, MPLS TE, IPv4 over IPv6 tunnel or manual IPv6 over IPv4 tunnel, 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, MPLS TE, 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.

You can configure a main interface working in Layer 3 mode as the source tunnel interface.

On the GRE, MPLS TE, IPv4 over IPv6 tunnel or manual IPv6 over IPv4 tunnel, the source address of the local tunnel interface is the destination address of the remote tunnel interface, and the destination address of the local tunnel interface is the source address of the remote tunnel interface.

## Example

# Set the tunnel type of Tunnel1 to IPv6 over IPv4 of manual mode and configure the source IP address of Tunnel1 as 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol ipv6-ipv4
[HUAWEI-Tunnel1] source 10.1.1.1
```

# Configure Tunnel1 of GRE and use Loopback1 address as the interface address.

```
<HUAWEI> system-view
[HUAWEI] interface Loopback 1
[HUAWEI-LoopBack1] ip address 10.2.1.1 32
[HUAWEI-LoopBack1] quit
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol gre
[HUAWEI-Tunnel1] source loopback 1
```

# 6.13.5 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** | **ipv6-ipv4** [ **6to4** | **isatap** ] | **ipv4-ipv6** | **mpls te** | **none** }

**undo tunnel-protocol**

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| **gre** | Indicate that the GRE tunnel protocol is configured on a tunnel interface.<br>**NOTE**<br>Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the parameters. | - |
| **ipv4-ipv6** | Indicate that the IPv4 to IPv6 tunnel protocol is configured on a tunnel interface.<br>**NOTE**<br>Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support the parameter. | - |
| **ipv6-ipv4** [ **6to4** \| **isatap** ] | Configure the tunnel protocol of the tunnel interface as ipv6-ipv4:<br>• **ipv6-ipv4**: use a manual IPv6 over IPv4 tunnel<br>• **ipv6-ipv4 6to4** : using 6to4 tunnel<br>• **ipv6-ipv4 isatap** : using isatap tunnel<br>**NOTE**<br>Only the S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support these parameter. | - |

| Parameter | Description | Value |
| --- | --- | --- |
| **mpls te** | Indicate that the MPLS TE tunnel protocol is configured on a tunnel interface.<br>**NOTE**<br>Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720-EI, S6720S-EI, S6730-H, S6730-S, S6730S-S, and S6730S-H support the parameter. | - |
| **none** | Indicate that no tunnel protocol is configured on a tunnel interface. | - |

## Views

Tunnel interface view

## 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.
- 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.
- 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.

**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.

### Example

# Set the tunnel encapsulation mode of Tunnel2 to GRE.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 2
[HUAWEI-Tunnel2] tunnel-protocol gre
```

# 6.14 IPv4 over IPv6 Tunnel Configuration Commands

## 6.14.1 Command Support

Only the following switch models support IPv4 over IPv6 Tunnel:

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S

## 6.14.2 display interface tunnel

### Function

The **display interface tunnel** command displays details of the tunnel interface.

### Format

**display interface tunnel** [ *interface-number* | **main** ]

### 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

### Usage Scenario

To check status of tunnels or diagnose the fault in these tunnels, run the **display interface tunnel** command. You can run this command to obtain tunnel interface information when configuring tunnels or when locating the fault on these tunnels.

### Prerequisites

Before run **display interface tunnel**, please ensure that tunnel interface has been created using the **interface tunnel** command.

## Example

# Display the details of the tunnel interface.

```
<HUAWEI> display interface tunnel 1
Tunnel1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2012-11-16 19:16:33 UTC+08:00
Description:
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 10.3.1.2/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.2.1.2 (Vlanif1234), destination 10.2.1.1
Tunnel protocol/transport GRE/IP, key disabled
keepalive enable period 5 retry-times 3
Checksumming of packets disabled
Current system time: 2012-11-16 19:17:39+08:00
Last 300 seconds input rate 16 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input:  5 packets, 650 bytes
Output:  0 packets, 0 bytes
   Input bandwidth utilization  :    0%
   Output bandwidth utilization :    0%
```

**Table 6-92** Description of the display interface tunnel command output

| Item | Description |
| --- | --- |
| Tunnel1 current state | Physical layer status of the tunnel interface:<br>● UP: The interface is in normal state.<br>● Administratively DOWN: The network administrator executes the **shutdown** command on the interface.<br>After a tunnel interface is created, its physical layer status is Up. |

| Item | Description |
| --- | --- |
| Line protocol current state | Link protocol status:<br>● UP: The link layer protocol of the tunnel interface works normally.<br>● Down: The link layer protocol of the tunnel interface is abnormal. |
| Last line protocol up time | Last time the link layer protocol of the tunnel interface goes UP.<br>**NOTE**<br>This field is displayed only when the link layer protocol status of the tunnel interface is UP. |
| Description | Description of the tunnel interface. |
| Route Port | Indicates the Layer 3 interface. |
| 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 Address is 10.3.1.2/24 | IP address of the tunnel interface is 10.3.1.2.<br>The mask is 24 bits, that is, 255.255.255.0. |
| Encapsulation is TUNNEL, | Encapsulation type of packets on a tunnel interface.<br>Packet encapsulation protects a whole IP packet. |
| loopback not set | The tunnel interface does not support a loopback test. |
| Tunnel source 10.2.1.2 (Vlanif1234) | The source address of the tunnel is 10.2.1.2. That is, the IP address of the VLANIF 1234 interface sending packets at the source side is 10.2.1.2. |
| destination 10.2.1.1 | Destination address of the tunnel. |
| Tunnel protocol/ transport GRE/IP, key disabled | The tunnel encapsulation protocol is the GRE protocol, and the transport protocol is the IP protocol.<br>Encapsulation protocol types of a tunnel are as follows:<br>● GRE: indicates Generic Routing Encapsulation.<br>● MPLS: encapsulates packets into MPLS packets.<br>● IPv6 over IPv4: encapsulates IPv6 packets into IPv4 packets.<br>● IPv4 over IPv6: encapsulates IPv4 packets into IPv6 packets.<br>● none: indicates no encapsulation. This is the default mode of the tunnel interface.<br>key disabled: the key word recognition function of GRE is not enabled. |

| Item | Description |
| --- | --- |
| keepalive enable period 5 retry-times 3 | The keepalive function of GRE. |
| Checksumming of packets disabled | The check sum function of GRE is not enabled. |
| Current system time | Current system time.<br>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. |
| 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 | Total number of received packets. |
| Output | Total number of sent packets. |
| Input bandwidth utilization : -- | Input bandwidth usage. |
| Output bandwidth utilization : -- | Output bandwidth usage. |

# 6.14.3 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 on embedded nodes of the IPv4 over IPv6 tunnel after an IPv4 packet is encapsulated the first time.

The **undo tunnel ipv4-ipv6 encapsulation-limit** command closes the function of IPv6 encapsulation on embedded nodes of the IPv4 over IPv6 tunnel.

By default, a maximum of four times of IPv6 encapsulation can be performed on embedded nodes of the IPv4 over IPv6 tunnel.

## 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 times for performing IPv6 encapsulation on embedded nodes of the IPv4 over IPv6 tunnel. | The value is an integer that ranges from 0 to 255. |

## Views

System view, tunnel interface view

## Default Level

2: Configuration level

## Usage Guidelines

**Usage Scenario**

The maximum number of times that IPv6 encapsulation can be performed on embedded nodes of the IPv4 over IPv6 tunnel 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.

**Prerequisites**

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.

**Precautions**

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 restore the maximum number of times that IPv6 encapsulation on embedded nodes of the IPv4 over IPv6 tunnel can be performed after an IPv4 packet is encapsulated the first time to the default value.

## Example

# Set the maximum number of times of IPv6 encapsulation to be performed on the embedded nodes of the specified IPv4 over IPv6 tunnel to 3.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol ipv4-ipv6
[HUAWEI-Tunnel1] tunnel ipv4-ipv6 encapsulation-limit 3
```

# Set the maximum number of times of IPv6 encapsulation to be performed on the embedded nodes of all specified IPv4 over IPv6 tunnels to 3 on the local device.

```
<HUAWEI> system-view
[HUAWEI] tunnel ipv4-ipv6 encapsulation-limit 3
```

## 6.14.4 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**

### 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 1
[HUAWEI-Tunnel1] tunnel-protocol ipv4-ipv6
[HUAWEI-Tunnel1] tunnel ipv4-ipv6 flow-label 10
```

# Set the flow label value of all the IPv4 over IPv6 tunnels on the local device to 10.

```
<HUAWEI> system-view
[HUAWEI] tunnel ipv4-ipv6 flow-label 10
```

# 6.14.5 tunnel ipv4-ipv6 hop-limit

## Function

The **tunnel ipv4-ipv6 hop-limit** command sets the hop limit of the IPv6 tunnel packets.

The **undo tunnel ipv4-ipv6 hop-limit** command restores the hop limit of the IPv6 tunnel packets to the default value.

By default, the hop limit of the IPv6 tunnel packets is 64.

## Format

**tunnel ipv4-ipv6 hop-limit** *hop-limit*

**undo tunnel ipv4-ipv6 hop-limit**

## Parameters

| Parameter | Description | Value |
| --- | --- | --- |
| *hop-limit* | Specifies the hop limit of the IPv6 tunnel packets. | The value is an integer that ranges from 1 to 255. |

## Views

system view, Tunnel interface view

## Default Level

2: Configuration level

## Usage Guidelines

Setting the hop limit of the IPv6 tunnel packets 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 1
[HUAWEI-Tunnel1] tunnel-protocol ipv4-ipv6
[HUAWEI-Tunnel1] tunnel ipv4-ipv6 hop-limit 100
```

# 6.14.6 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.

## 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 IPv4 over IPv6 tunnel header uses the value in Traffic Class field of the original packet. | - |
| *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

### Usage Scenario

The traffic level of the IPv4 over 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.

### Prerequisites

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.

### Precautions

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 specified IPv4 over IPv6 tunnel to 10.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol ipv4-ipv6
[HUAWEI-Tunnel1] tunnel ipv4-ipv6 traffic-class 10
```

# Set the traffic level of all the IPv4 over IPv6 tunnels on the local device to 10.

```
<HUAWEI> system-view
[HUAWEI] tunnel ipv4-ipv6 traffic-class 10
```