HP 5120 SI Switch Series

Layer 3 - IP Services

Command Reference

Part number: 5998-1810
Software version: Release 1513
Document version: 6W100-20130830

Legal and notice information

The information contained herein is subject to change without notice.

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Contents

ARP configuration commands

arp check enable

Syntax

arp check enable

undo arp check enable

View

System view

Default level

2: System level

Parameters

None

Description

Use the **arp check enable** command to enable dynamic ARP entry check.

Use the **undo arp check enable** command to disable dynamic ARP entry check.

By default, dynamic ARP entry check is enabled.

Examples

Enable ARP entry check.

```
<Sysname> system-view
[Sysname] arp check enable
```

arp max-learning-num

Syntax

arp max-learning-num *number*

undo arp max-learning-num

View

Ethernet interface view, VLAN interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

number: Maximum number of dynamic ARP entries that an interface can learn, in the range 0 to 256.

Description

Use the **arp max-learning-num** command to configure the maximum number of dynamic ARP entries that an interface can learn.

Use the **undo arp max-learning-num** command to restore the default.

By default, the maximum number of dynamic ARP entries that an interface can learn is 256.

When the *number* argument is set to 0, the interface is disabled from learning dynamic ARP entries.

Examples

Specify VLAN-interface 40 to learn up to 50 dynamic ARP entries.

```
<Sysname> system-view
[Sysname] interface vlan-interface 40
[Sysname-Vlan-interface40] arp max-learning-num 50
```

Specify GigabitEthernet 1/0/1 to learn up to 100 dynamic ARP entries.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp max-learning-num 100
```

Specify Layer 2 aggregate interface bridge-aggregation 1 to learn up to 100 dynamic ARP entries.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] arp max-learning-num 100
```

arp static

Syntax

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

undo arp static *ip-address*

undo arp *ip-address*

View

System view

Default level

2: System level

Parameters

ip-address: IP address in an ARP entry.

mac-address: MAC address in an ARP entry, in the format H-H-H.

vlan-id: ID of a VLAN to which a static ARP entry belongs to, in the range 1 to 4094.

interface-type interface-number: Interface type and interface number.

Description

Use the **arp static** command to configure a static ARP entry in the ARP mapping table.

Use the **undo arp** command to remove an ARP entry.

NOTE:

- A static ARP entry is effective when the switch works normally. However, when the VLAN or VLAN interface to which an ARP entry corresponds is deleted, the entry, if long, will be deleted, and if short and resolved, will become unresolved.
- The *vlan-id* argument specifies the VLAN corresponding to an ARP entry and must be the ID of an existing VLAN. In addition, the Ethernet interface following the argument must belong to that VLAN. The VLAN interface of the VLAN must have been created.
- If both the *vlan-id* and *ip-address* arguments are specified, the IP address of the VLAN interface corresponding to the *vlan-id* argument must belong to the same network segment as the IP address specified by the *ip-address* argument.

Related commands: **reset arp** and **display arp**.

Examples

Configure a static ARP entry, with the IP address being 202.38.10.2, the MAC address being 00e0-fc01-0000, and the outbound interface being GigabitEthernet 1/0/1 of VLAN 10.

```
<Sysname> system-view
[Sysname] arp static 202.38.10.2 00e0-fc01-0000 10 GigabitEthernet 1/0/1
```

arp timer aging

Syntax

arp timer aging *aging-time*

undo arp timer aging

View

System view

Default level

2: System level

Parameters

aging-time: Aging time for dynamic ARP entries in minutes, in the range 1 to 1,440.

Description

Use the **arp timer aging** command to set aging time for dynamic ARP entries.

Use the **undo arp timer aging** command to restore the default.

By default, the aging time for dynamic ARP entries is 20 minutes.

Related commands: **display arp timer aging**.

Examples

Set aging time for dynamic ARP entries to 10 minutes.

```
<Sysname> system-view
[Sysname] arp timer aging 10
```

display arp

Syntax

display arp [[**all** | **dynamic** | **static**] [**slot** *slot-number*] | **vlan** *vlan-id* | **interface** *interface-type interface-number*] [**count**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

all: Displays all ARP entries.

dynamic: Displays dynamic ARP entries.

static: Displays static ARP entries.

slot *slot-number*: Displays the ARP entries of the specified device. If the device is in an IRF, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF, the *slot-number* argument represents the current device ID.

vlan *vlan-id*: Displays the ARP entries of the specified VLAN. The VLAN ID ranges from 1 to 4,094.

interface *interface-type interface-number:* Displays the ARP entries of the interface specified by the argument *interface-type interface-number*.

count: Displays the number of ARP entries.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display arp** command to display ARP entries in the ARP mapping table.

If no parameter is specified, all ARP entries are displayed.

Related commands: **arp static** and **reset arp**.

Examples

Display the detailed information of all ARP entries.

```
<Sysname> display arp all
                Type: S-Static    D-Dynamic
IP Address       MAC Address     VLAN ID  Interface             Aging Type
192.168.1.1      00e0-fc01-0000  10       GE1/0/1               N/A   S
192.168.0.254    00e0-fc00-5112  1        GE1/0/45              19    D
192.168.0.235    00e0-fc02-2181  1        GE1/0/45              20    D
192.168.0.5      00e0-4c3d-35d7  1        GE1/0/45              19    D
192.168.0.108    000d-88f6-44c1  1        GE1/0/45              14    D
```

```
192.168.0.2      000d-88f7-b090  1        GE1/0/45              6     D
192.168.0.16     0015-e943-7326  1        GE1/0/45              2     D
192.168.0.3      000d-88f8-4e71  1        GE1/0/45              12    D
192.168.0.7      0021-86f9-602c  1        GE1/0/45              10    D
192.168.0.6      0015-e943-712f  1        GE1/0/45              3     D
192.168.0.18     0021-86f9-044c  1        GE1/0/45              20    D
192.168.0.71     000f-e234-5679  1        GE1/0/45              6     D
```

Table 1 Output description

Field	Description
IP Address	IP address in an ARP entry
MAC Address	MAC address in an ARP entry
VLAN ID	VLAN ID contained a static ARP entry
Interface	Outbound interface in an ARP entry
Aging	Aging time for a dynamic ARP entry in minutes ("DIS" or "N/A" means unknown aging time or no aging time)
Type	ARP entry type: D for dynamic, S for static

Display the number of all ARP entries.

```
<Sysname> display arp all count
 Total Entry(ies):  12
```

display arp *ip-address*

Syntax

display arp *ip-address* [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

ip-address: Displays the ARP entry for the specified IP address.

slot *slot-number*: Displays the ARP entries of the specified device. The *slot-number* argument is the member number of the device in the IRF, which you can display with the **display irf** command. The value range for the *slot-number* argument depends on the number of members and numbering conditions in the current IRF. If no IRF exists, the *slot-number* argument is the current device number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display arp** *ip-address* command to display the ARP entry for a specified IP address.

Related commands: **arp static** and **reset arp**.

Examples

Display the corresponding ARP entry for the IP address 20.1.1.1.

```
<Sysname> display arp 20.1.1.1
                Type: S-Static    D-Dynamic
IP Address       MAC Address     VLAN ID  Interface             Aging Type
20.1.1.1         00e0-fc00-0001  N/A      N/A                   N/A   S
```

display arp timer aging

Syntax

display arp timer aging [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display arp timer aging** command to display the age timer for dynamic ARP entries.

Related commands: **arp timer aging**.

Examples

Display the age timer for dynamic ARP entries.

```
<Sysname> display arp timer aging
Current ARP aging time is 10 minute(s)
```

reset arp

Syntax

reset arp { **all** | **dynamic** | **static** | **slot** *slot-number* | **interface** *interface-type interface-number* }

View

User view

Default level

2: System level

Parameters

all: Clears all ARP entries.

dynamic: Clears all dynamic ARP entries.

static: Clears all static ARP entries.

slot *slot-number*: Clears the ARP entries for the specified device. The *slot-number* argument is the member number of the device in the IRF, which you can display with the **display irf** command. The value range for the *slot-number* argument depends on the number of members and numbering conditions in the current IRF. If no IRF exists, the *slot-number* argument is the current device number.

interface *interface-type interface-number*: Clears the ARP entries for the interface specified by the argument *interface-type interface-number*.

Description

Use the **reset arp** command to clear ARP entries from the ARP mapping table.

Related commands: **arp static** and **display arp**.

Examples

Clear all static ARP entries.

```
<Sysname> reset arp static
```

Gratuitous ARP configuration commands

arp send-gratuitous-arp

Syntax

arp send-gratuitous-arp [**interval** *milliseconds*]

undo arp send-gratuitous-arp

View

VLAN interface view

Default level

2: System level

Parameters

interval *milliseconds*: Sets the interval at which gratuitous ARP packets are sent, in the range 200 to 200000 milliseconds. The default value is 2000.

Description

Use the **arp send-gratuitous-arp** command to enable periodic sending of gratuitous ARP packets and set the sending interval for the interface.

Use the **undo arp send-gratuitous-arp** command to disable the interface from periodically sending gratuitous ARP packets.

By default, an interface is disabled from sending gratuitous ARP packets periodically.

- This function takes effect only when the link of the enabled interface goes up and an IP address has been assigned to the interface.
- If you change the interval for sending gratuitous ARP packets, the configuration is effective at the next sending interval.
- The frequency of sending gratuitous ARP packets may be much lower than is expected if this function is enabled on multiple interfaces, or each interface is configured with multiple secondary IP addresses, or a small sending interval is configured in the preceding cases.

Examples

Enable VLAN-interface 2 to send gratuitous ARP packets every 300 milliseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] arp send-gratuitous-arp interval 300
```

arp ip-conflict prompt

Syntax

arp ip-conflict prompt

undo arp ip-conflict prompt

View

System view

Default level

2: System level

Description

Use **arp ip-conflict prompt** to enable IP conflict notification.

Use **undo arp ip-conflict prompt** to restore the default.

By default, this function is disabled.

Examples

Enable IP conflict notification.

```
<Sysname> system-view
[Sysname] arp ip-conflict prompt
```

gratuitous-arp-sending enable

Syntax

gratuitous-arp-sending enable

undo gratuitous-arp-sending enable

View

System view

Default level

2: System level

Parameters

None

Description

Use the **gratuitous-arp-sending enable** command to enable a switch to send gratuitous ARP packets when receiving ARP requests from another network segment.

Use the **undo gratuitous-arp-sending enable** command to restore the default.

By default, a switch cannot send gratuitous ARP packets when receiving ARP requests from another network segment.

Examples

Disable a switch from sending gratuitous ARP packets.

```
<Sysname> system-view
[Sysname] undo gratuitous-arp-sending enable
```

gratuitous-arp-learning enable

Syntax

gratuitous-arp-learning enable

undo gratuitous-arp-learning enable

View

System view

Default level

2: System level

Parameters

None

Description

Use the **gratuitous-arp-learning enable** command to enable the gratuitous ARP packet learning function.

Use the **undo gratuitous-arp-learning enable** command to disable the function.

By default, the function is enabled.

With this function enabled, a switch receiving a gratuitous ARP packet can add the source IP and MAC addresses carried in the packet to its own dynamic ARP table if it finds no ARP entry in the cache corresponding to the source IP address of the ARP packet exists; if the corresponding ARP entry exists in the cache, the switch updates the ARP entry regardless of whether this function is enabled.

Examples

Enable the gratuitous ARP packet learning function.

```
<Sysname> system-view
[Sysname] gratuitous-arp-learning enable
```

ARP snooping configuration commands

arp-snooping enable

Syntax

arp-snooping enable

undo arp-snooping enable

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use the **arp-snooping enable** command to enable ARP snooping.

Use the **undo arp-snooping enable** command to disable ARP snooping.

By default, ARP snooping is disabled.

Examples

Enable ARP snooping on VLAN 1.

```
<Sysname> system-view
[Sysname] vlan 1
[Sysname-vlan1] arp-snooping enable
```

display arp-snooping

Syntax

display arp-snooping [**ip** *ip-address* | **vlan** *vlan-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

ip *ip-address*: Displays the ARP snooping entry for a specific IP address.

vlan *vlan-id*: Displays ARP snooping entries of a specific VLAN. The *vlan-id* argument is in the range of 1 to 4094.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display arp-snooping** command to display ARP snooping entries. If no keywords or arguments are specified, the command displays all ARP snooping entries.

Examples

Display ARP snooping entries of VLAN 1.

```
<Sysname> display arp-snooping vlan 1
IP Address    MAC Address    VLAN ID Interface  Aging       Status
3.3.3.3       0003-0003-0003 1       GE1/0/1     20          Valid
3.3.3.4       0004-0004-0004 1       GE1/0/2     5           Invalid
---- Total entry(ies) on VLAN 1:2 ----
```

reset arp-snooping

Syntax

reset arp-snooping [**ip** *ip-address* | **vlan** *vlan-id*]

View

User view

Default level

2: System level

Parameters

ip *ip-address*: Removes the ARP snooping entry of a specific IP address.

vlan *vlan-id*: Removes the ARP snooping entries of a specific VLAN. The *vlan-id* argument is in the range of 1 to 4094.

Description

Use the **reset arp-snooping** command to remove ARP snooping entries. If no keywords or arguments are specified, the command removes all ARP snooping entries.

Examples

Remove ARP snooping entries of VLAN 1.

```
<Sysname> reset arp-snooping vlan 1
```

IP addressing configuration commands

display ip interface

Syntax

display ip interface [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display ip interface** command to display IP configuration information for a specified Layer 3 interface or all Layer 3 interfaces.

Examples

Display IP configuration information for interface VLAN-interface 1.

```
<Sysname> display ip interface vlan-interface 1
Vlan-interface1 current state :DOWN
Line protocol current state :DOWN
Internet Address is 1.1.1.1/8 Primary
Broadcast address : 1.255.255.255
The Maximum Transmit Unit : 1500 bytes
input packets : 0, bytes : 0, multicasts : 0
output packets : 0, bytes : 0, multicasts : 0
ARP packet input number:           0
  Request packet:                  0
  Reply packet:                    0
  Unknown packet:                  0
TTL invalid packet number:         0
ICMP packet input number:          0
  Echo reply:                      0
  Unreachable:                     0
```

```
Source quench:                  0
Routing redirect:               0
Echo request:                   0
Router advert:                  0
Router solicit:                 0
Time exceed:                    0
IP header bad:                  0
Timestamp request:              0
Timestamp reply:                0
Information request:            0
Information reply:              0
Netmask request:                0
Netmask reply:                  0
Unknown type:                   0
```

Table 2 Output description

Field	Description
current state	Current physical state of the interface, which can be • Administrative DOWN: Indicates that the interface is administratively down. The interface is shut down with the **shutdown** command. • DOWN: Indicates that the interface is administratively up but its physical state is down, which may be caused by a connection or link failure. • UP: Indicates that both the administrative and physical states of the interface are up.
Line protocol current state	Current state of the link layer protocol, which can be • DOWN: Indicates that the protocol state of the interface is down. • UP: Indicates that the protocol state of the interface is up. • UP (spoofing): Indicates that the protocol state of the interface pretends to be up; however, no corresponding link is present, or the corresponding link is not present permanently but is established as needed.
Internet Address	IP address of an interface followed by: • Primary: Identifies a primary IP address. • acquired via DHCP: Identifies an IP address obtained through DHCP. • acquired via BOOTP: Identifies an IP address obtained through BOOTP.
Broadcast address	Broadcast address of the subnet attached to an interface
The Maximum Transmit Unit	Maximum transmission units on the interface, in bytes
input packets, bytes, multicasts output packets, bytes, multicasts	Unicast packets, bytes, and multicast packets received on an interface (the statistics start at the switch startup)
ARP packet input number: Request packet: Reply packet: Unknown packet:	Total number of ARP packets received on the interface (the statistics start at the switch startup), including • ARP request packets • ARP reply packets • Unknown packets

Field	Description
TTL invalid packet number	Number of TTL-invalid packets received on the interface (the statistics start at the switch startup)
ICMP packet input number: Echo reply: Unreachable: Source quench: Routing redirect: Echo request: Router advert: Router solicit: Time exceed: IP header bad: Timestamp request: Timestamp reply: Information request: Information reply: Netmask request: Netmask reply: Unknown type:	Total number of ICMP packets received on the interface (the statistics start at the switch startup), including the following packets: • Echo reply packets • Unreachable packets • Source quench packets • Routing redirect packets • Echo request packets • Router advertisement packets • Router solicitation packets • Time exceeded packets • IP header bad packets • Timestamp request packets • Timestamp reply packets • Information request packets • Information reply packets • Netmask request packets • Netmask reply packets • Unknown type packets

display ip interface brief

Syntax

display ip interface [*interface-type* [*interface-number*]] **brief** [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface-type: Interface type.

interface-number: Interface number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display ip interface brief** command to display brief IP configuration information for a specified Layer 3 interface or all Layer 3 interfaces.

Note that:

- Without the interface type and interface number specified, the brief IP configuration information for all Layer 3 interfaces is displayed.
- With only the interface type specified, the brief IP configuration information for all Layer 3 interfaces of the specified type is displayed.
- With both the interface type and interface number specified, only the brief IP configuration information for the specified interface is displayed.

Related commands: **display ip interface**.

Examples

Display brief IP configuration information for VLAN interfaces.

```
<Sysname> display ip interface vlan-interface brief
*down: administratively down
(s): spoofing
Interface                  Physical Protocol IP Address      Description
Vlan-interface1            up       up       6.6.6.6         Vlan-inte...
Vlan-interface2            up       up       7.7.7.7         VLAN2
```

Table 3 Output description

Field	Description
*down: administratively down	The interface is administratively shut down with the **shutdown** command.
(s) : spoofing	Spoofing attribute of the interface. It indicates that an interface whose link layer protocol is displayed up may have no link present or the link is set up only on demand.
Interface	Interface name
Physical	Physical state of the interface, which can be • *down: Indicates that the interface is administratively down. The interface is shut down with the **shutdown** command. • down: Indicates that the interface is administratively up but its physical state is down, which may be caused by a connection or link failure. • up: Indicates that both the administrative and physical states of the interface are up.
Protocol	Link layer protocol state of the interface, which can be • down: Indicates that the protocol state of the interface is down. • up: Indicates that the protocol state of the interface is up. • up(s): Indicates that the protocol state of the interface is up (spoofing).
IP Address	IP address of the interface (If no IP address is configured, "unassigned" is displayed.)
Description	Interface description information, for which at most 12 characters can be displayed. If there are more that 12 characters, only the first nine characters are displayed.

ip address

Syntax

ip address *ip-address* { *mask-length* | *mask* }

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

View

Interface view

Default level

2: System level

Parameters

ip-address: IP address of interface, in dotted decimal notation.

mask-length: Subnet mask length, the number of consecutive ones in the mask.

mask: Subnet mask in dotted decimal notation.

Description

Use the **ip address** command to assign an IP address and mask to the interface.

Use the **undo ip address** command to remove all IP addresses from the interface.

Use the **undo ip address** *ip-address* { *mask* | *mask-length* } command to remove the IP address.

By default, no IP address is assigned to any interface.

Related commands: **display ip interface**.

Examples

Assign VLAN-interface 1 an IP address 129.12.0.1, with subnet masks being 255.255.255.0.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip address 129.12.0.1 255.255.255.0
```

DHCP server configuration commands

NOTE:

The DHCP server configuration is supported only on VLAN interfaces, and loopback interfaces. The subaddress pool configuration is not supported on loopback interfaces.

bims-server

Syntax

bims-server ip *ip-address* [**port** *port-number*] **sharekey** [**cipher** | **simple**] *key*

undo bims-server

View

DHCP address pool view

Default level

2: System level

Parameters

ip *ip-address*: Specifies an IP address for the BIMS server.

port *port-number*: Specifies a port number for the BIMS server in the range 1 to 65534.

cipher: Sets a ciphertext key.

simple: Sets a plaintext key.

key: Specifies the key string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 16 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 53 characters. If neither **cipher** nor **simple** is specified, you set a plaintext key string.

Description

Use the **bims-server** command to specify the IP address, port number, and shared key of the BIMS server in the DHCP address pool for the client.

Use the **undo bims-server** command to remove the specified BIMS server information.

By default, no BIMS server information is specified.

If you execute the **bims-server** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool** and **display dhcp server tree**.

Examples

Specify the IP address 1.1.1.1, port number 80, shared key aabbcc of the BIMS server in DHCP address pool 0 for the client.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] bims-server ip 1.1.1.1 port 80 sharekey simple aabbcc
```

bootfile-name

Syntax

bootfile-name *bootfile-name*

undo bootfile-name

View

DHCP address pool view

Default level

2: System level

Parameters

bootfile-name: Boot file name, a string of 1 to 63 characters.

Description

Use the **bootfile-name** command to specify a bootfile name in the DHCP address pool for the client.

Use the **undo bootfile-name** command to remove the specified bootfile name.

By default, no bootfile name is specified.

If you execute the **bootfile-name** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool** and **display dhcp server tree**.

Examples

Specify the bootfile name **aaa.cfg** in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] bootfile-name aaa.cfg
```

dhcp enable

Syntax

dhcp enable

undo dhcp enable

View

System view

Default level

2: System level

Parameters

None

Description

Use the **dhcp enable** command to enable DHCP.

Use the **undo dhcp enable** command to disable DHCP.

By default, DHCP is disabled.

NOTE:

You need to enable DHCP before performing DHCP server and relay agent configurations.

Examples

Enable DHCP.

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

dhcp server apply ip-pool

Syntax

dhcp server apply ip-pool *pool-name*

undo dhcp server apply ip-pool [*pool-name*]

View

Interface view

Default level

2: System level

Parameters

pool-name: DHCP address pool name, a case-insensitive string in the range of 1 to 35 characters.

Description

Use the **dhcp server apply ip-pool** command to apply an extended address pool on an interface.

Use the **undo dhcp server apply ip-pool** command to remove the configuration.

By default, no extended address pool is applied on an interface, and the server assigns an IP address from a common address pool to a client when the client's request arrives at the interface.

If you execute the **dhcp server apply ip-pool** command on an interface, when a client's request arrives at the interface, the server attempts to assign the client the statically bound IP address first and then an IP address from this extended address pool.

Only an extended address pool can be applied on an interface. The address pool to be referenced must already exist.

Related commands: **dhcp server ip-pool**.

Examples

Apply extended DHCP address pool 0 on VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp server apply ip-pool 0
```

dhcp select server global-pool

Syntax

dhcp select server global-pool [**subaddress**]

undo dhcp select server global-pool [**subaddress**]

View

Interface view

Default level

2: System level

Parameters

subaddress: Supports secondary address allocation. When the DHCP server and client are on the same network segment, the server preferably assigns an IP address from an address pool that resides on the same subnet as the primary IP address of the server interface (connecting to the client). If the address pool contains no assignable IP address, the server assigns an IP address from an address pool that resides on the same subnet as the secondary IP addresses of the server interface. If the interface has multiple secondary IP addresses, each address pool is tried in turn for address allocation. Without the keyword **subaddress** specified, the DHCP server can only assign an IP address from the address pool that resides on the same subnet as the primary IP address of the server interface.

Description

Use the **dhcp select server global-pool** command to enable the DHCP server on specified interface(s). After the interface receives a DHCP request from a client, the DHCP server will allocate an IP address from the address pool.

Use the **undo dhcp select server global-pool** command to remove the configuration. Upon receiving a DHCP request from a client, the interface will neither assign an IP address to the client, nor serve as a DHCP relay agent to forward the request.

Use the **undo dhcp select server global-pool subaddress** command to disable the support for secondary address allocation.

By default, the DHCP server is enabled on an interface.

Examples

Enable the DHCP server on VLAN-interface 1 to assign IP addresses from the address pool that resides on the same subnet as the primary IP address of the server interface (connecting to the client) for the client.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp select server global-pool
```

dhcp server detect

Syntax

dhcp server detect

undo dhcp server detect

View

System view

Default level

2: System level

Parameters

None

Description

Use the **dhcp server detect** command to enable unauthorized DHCP server detection.

Use the **undo dhcp server detect** command to disable the function.

By default, the function is disabled.

With this function enabled, upon receiving a DHCP request, the DHCP server will resolve from the request the IP addresses of DHCP servers which ever offered IP addresses to the DHCP client and the receiving interface. Each server detected is recorded only once. The administrator can get this information from logs to check out unauthorized DHCP servers.

Examples

Enable unauthorized DHCP server detection.

```
<Sysname> system-view
[Sysname] dhcp server detect
```

dhcp server forbidden-ip

Syntax

dhcp server forbidden-ip *low-ip-address* [*high-ip-address*]

undo dhcp server forbidden-ip *low-ip-address* [*high-ip-address*]

View

System view

Default level

2: System level

Parameters

low-ip-address: Start IP address of the IP address range to be excluded from dynamic allocation.

high-ip-address: End IP address of the IP address range to be excluded from dynamic allocation. The end IP address must have a higher sequence than the start one.

Description

Use the **dhcp server forbidden-ip** command to exclude IP addresses from dynamic allocation.

Use the **undo dhcp server forbidden-ip** command to remove the configuration.

By default, all IP addresses in a DHCP address pool are assignable except IP addresses of the DHCP server interfaces.

- When you use the **dhcp server forbidden-ip** command to exclude an IP address that is bound to a user from dynamic assignment, the address can be still assigned to the user.
- When you use the **undo dhcp server forbidden-ip** command to remove the configuration, the specified address/address range must be consistent with the one specified with the **dhcp server forbidden-ip** command. If you have configured to exclude an address range from dynamic assignment, you need to specify the same address range in the **undo dhcp server forbidden-ip** command instead of specifying one IP address.
- Using the **dhcp server forbidden-ip** command repeatedly can exclude multiple IP address ranges from allocation.

Related commands: **display dhcp server forbidden-ip**, **dhcp server ip-pool**, **network**, and **static-bind ip-address**.

Examples

Exclude the IP address range 10.110.1.1 to 10.110.1.63 from dynamic allocation.

```
<Sysname> system-view
[Sysname] dhcp server forbidden-ip 10.110.1.1 10.110.1.63
```

dhcp server ip-pool

Syntax

dhcp server ip-pool *pool-name* [**extended**]

undo dhcp server ip-pool *pool-name*

View

System view

Default level

2: System level

Parameters

pool-name: Global address pool name, which is a unique pool identifier, a string of 1 to 35 characters.

extended: Specifies the address pool as an extended address pool. If this keyword is not specified, the address pool is a common address pool.

Description

Use the **dhcp server ip-pool** command to create a DHCP address pool and enter its view. If the pool was created, you will directly enter its view.

Use the **undo dhcp server ip-pool** command to remove the specified DHCP address pool.

By default, no DHCP address pool is created.

Related commands: **dhcp enable** and **display dhcp server tree**.

Examples

Create the common address pool identified by 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0]
```

dhcp server ping packets

Syntax

dhcp server ping packets *number*

undo dhcp server ping packets

View

System view

Default level

2: System level

Parameters

number: Number of ping packets, in the range of 0 to 10. 0 means no ping operation.

Description

Use the **dhcp server ping packets** command to specify the maximum number of ping packets on the DHCP server.

Use the **undo dhcp server ping packets** command to restore the default.

The number defaults to 1.

Examples

Specify the maximum number of ping packets as 10.

```
<Sysname> system-view
[Sysname] dhcp server ping packets 10
```

dhcp server ping timeout

Syntax

dhcp server ping timeout *milliseconds*

undo dhcp server ping timeout

View

System view

Default level

2: System level

Parameters

milliseconds: Response timeout value for ping packets in milliseconds, in the range of 0 to 10,000. 0 means no ping operation.

Description

Use the **dhcp server ping timeout** command to configure response timeout time of the ping packet on the DHCP server.

Use the **undo dhcp server ping timeout** command to restore the default.

The time defaults to 500 ms.

Examples

Specify the response timeout time as 1000 ms.

```
<Sysname> system-view
[Sysname] dhcp server ping timeout 1000
```

dhcp server relay information enable

Syntax

dhcp server relay information enable

undo dhcp server relay information enable

View

System view

Default level

2: System level

Parameters

None

Description

Use the **dhcp server relay information enable** command to enable the DHCP server to handle Option 82.

Use the **undo dhcp server relay information enable** command to configure the DHCP server to ignore Option 82.

By default, the DHCP server handles Option 82.

Examples

Configure the DHCP server to ignore Option 82.

```
<Sysname> system-view
[Sysname] undo dhcp server relay information enable
```

dhcp server threshold

Syntax

dhcp server threshold { **allocated-ip** *threshold-value* | **average-ip-use** *threshold-value* | **max-ip-use** *threshold-value* }

undo dhcp server threshold { **allocated-ip** | **average-ip-use** | **max-ip-use** }

View

System view

Default level

2: System level

Parameters

allocated-ip *threshold-value*: Enables the DHCP server to send trap messages to the network management server when the ratio of successfully allocated IP addresses to received DHCP requests within five minutes reaches the threshold specified by the *threshold-value* argument. The threshold is a percentage value ranging from 1 to 100.

average-ip-use *threshold-value*: Enables the DHCP server to send trap messages to the network management server when the average IP address utilization of an address pool within five minutes reaches the threshold specified by the *threshold-value* argument. The threshold is a percentage value ranging from 1 to 100.

max-ip-use *threshold-value*: Enables the DHCP server to send trap messages to the network management server when the maximum IP address utilization of an address pool within five minutes reaches the threshold specified by the *threshold-value* argument. The threshold is a percentage value ranging from 1 to 100.

Description

Use the **dhcp server threshold** command to enable the DHCP server to send trap messages to the network management server when the specified threshold is reached.

Use the **undo dhcp server threshold** command to restore the default.

By default, the DHCP server does not send trap messages to the network management server.

Examples

Enable the DHCP server to send trap messages to the network management server when the ratio of successfully allocated IP addresses to received DHCP requests within five minutes exceeds 50%.

```
<Sysname> system-view
[Sysname] dhcp server threshold allocated-ip 50
```

Enable the DHCP server to send trap messages to the network management server when the average IP address utilization of an address pool within five minutes exceeds 80%.

```
<Sysname> system-view
[Sysname] dhcp server threshold average-ip-use 80
```

Enable the DHCP server to send trap messages to the network management server when the maximum IP address utilization of an address pool within five minutes exceeds 80%.

```
<Sysname> system-view
[Sysname] dhcp server threshold max-ip-use 80
```

display dhcp server conflict

Syntax

display dhcp server conflict { **all** | **ip** *ip-address* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

all: Displays information about all IP address conflicts.

ip-address: Displays conflict information for a specified IP address.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display dhcp server conflict** command to display information about IP address conflicts.

Related commands: **reset dhcp server conflict**.

Examples

Display information about all IP address conflicts.

```
<Sysname> display dhcp server conflict all
    Address             Discover time
    4.4.4.1             Apr 25 2007 16:57:20
```

```
   4.4.4.2             Apr 25 2007 17:00:10
--- total 2 entry ---
```

Table 4 Output description

Field	Description
Address	Conflicted IP address
Discover Time	Time when the conflict was discovered

display dhcp server expired

Syntax

display dhcp server expired { **all** | **ip** *ip-address* | **pool** [*pool-name*] } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

all: Displays the lease expiration information of all DHCP address pools.

ip *ip-address*: Displays the lease expiration information of a specified IP address.

pool [*pool-name*]: Displays the lease expiration information of a specified address pool. The *pool name* is a string of 1 to 35 characters. If the *pool name* is not specified, the lease expiration information of all address pools is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display dhcp server expired** command to display the lease expiration information of specified DHCP address pool(s) or an IP address.

DHCP will assign these expired IP addresses to DHCP clients after all addresses have been assigned.

Examples

Display information about lease expirations in all DHCP address pools.

```
<Sysname> display dhcp server expired all
 IP address       Client-identifier/    Lease expiration          Type
                    Hardware address
 4.4.4.6          3030-3066-2e65-3230-  Apr 25 2007 17:10:47     Release
                   302e-3130-3234-2d45-
                   7468-6572-6e65-7430-
```

```
                    2f31

--- total 1 entry ---
```

Table 5 Output description

Field	Description
IP address	Expired IP addresses.
Client-identifier/Hardware address	IDs or MACs of clients whose IP addresses were expired.
Lease expiration	The lease expiration time.
Type	Types of lease expirations. This field is set to Release.

display dhcp server free-ip

Syntax

display dhcp server free-ip [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display dhcp server free-ip** command to display information about assignable IP addresses which have never been assigned.

Examples

Display information about assignable IP addresses.

```
<Sysname> display dhcp server free-ip
IP Range from 10.0.0.0              to  10.0.0.255
```

display dhcp server forbidden-ip

Syntax

display dhcp server forbidden-ip [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display dhcp server forbidden-ip** command to display IP addresses excluded from dynamic allocation in DHCP address pool.

Examples

Display IP addresses excluded from dynamic allocation in the DHCP address pool.

```
<Sysname> display dhcp server forbidden-ip
Global:
IP Range from 1.1.0.2              to  1.1.0.3
IP Range from 1.1.1.2              to  1.1.1.3
Pool name: 2
1.1.1.5          1.1.1.6
```

Table 6 Output description

Field	Description
Global	Globally excluded IP addresses specified with the **dhcp server forbidden-ip** command in system view. No address pool can assign these IP addresses.
Pool name	Excluded IP addresses specified with the **forbidden-ip** command in DHCP address pool view. They cannot be assigned from the current extended address pool only.

display dhcp server ip-in-use

Syntax

display dhcp server ip-in-use { **all** | **ip** *ip-address* | **pool** [*pool-name*] } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

all: Displays the binding information of all DHCP address pools.

ip *ip-address*: Displays the binding information of a specified IP address.

pool [*pool-name*]: Displays the binding information of a specified address pool. The *pool name* is a string of 1 to 35 characters. If no *pool name* is specified, the binding information of all address pools is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display dhcp server ip-in-use** command to display the binding information of DHCP address pool(s) or an IP address.

Related commands: **reset dhcp server ip-in-use**.

Examples

Display the binding information of all DHCP address pools.

```
<Sysname> display dhcp server ip-in-use all
Pool utilization: 0.39%
 IP address    Client-identifier/    Lease expiration        Type
                  Hardware address
 10.1.1.1       4444-4444-4444        NOT Used                  Manual
 10.1.1.2      3030-3030-2e30-3030-   May  1 2009 14:02:49     Auto:COMMITTED
               662e-3030-3033-2d45-
               7468-6572-6e65-7430-
               2f31

 --- total 2 entry ---
```

Table 7 Output description

Field	Description
Pool utilization	Utilization rate of IP addresses in a DHCP address pool, which is the ratio of assigned IP addresses to assignable IP addresses in the DHCP address pool. • When the binding information of all DHCP address pools is displayed, this field displays the total utilization rate of IP addresses in all DHCP address pools. • When the binding information of a specific DHCP address pool is displayed, this field displays the utilization rate of IP addresses in the DHCP address pool. • When the binding information of a specific IP address is displayed, this field is not displayed.
IP address	Bound IP address
Client-identifier/Hardware address	Client's ID or MAC of the binding

Field	Description
Lease expiration	Lease expiration time, which can be • Specific time (May 1 2009 14:02:49 in this example): Time when the lease expires • NOT Used: The IP address of the static binding has not been assigned to the specific client. • Unlimited: Infinite lease expiration time
Type	Binding types, including Manual, Auto:OFFERED and Auto:COMMITTED. • Manual: Static binding • Auto:OFFERED: The binding sent in the DHCP-OFFER message from the server to the client. • Auto:COMMITTED: The binding sent in the DHCP-ACK message from the server to the client.

display dhcp server statistics

Syntax

display dhcp server statistics [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display dhcp server statistics** command to display the statistics of the DHCP server.

Related commands: **reset dhcp server statistics**.

Examples

Display the statistics on the DHCP server.

```
<Sysname> display dhcp server statistics
    Global Pool:
      Pool Number:                    1
      Binding:
        Auto:                         1
        Manual:                       0
        Expire:                       0
```

```
  BOOTP Request:                  10
    DHCPDISCOVER:                 5
    DHCPREQUEST:                  3
    DHCPDECLINE:                  0
    DHCPRELEASE:                  2
    DHCPINFORM:                   0
    BOOTPREQUEST:                 0
  BOOTP Reply:                    6
    DHCPOFFER:                    3
    DHCPACK:                      3
    DHCPNAK:                      0
    BOOTPREPLY:                   0
  Bad Messages:                   0
```

Table 8 Output description

Field	Description
Global Pool	Statistics of a DHCP address pool
Pool Number	The number of address pools
Auto	The number of dynamic bindings
Manual	The number of static bindings
Expire	The number of expired bindings
BOOTP Request	The number of DHCP requests sent from DHCP clients to the DHCP server, including: • DHCPDISCOVER • DHCPREQUEST • DHCPDECLINE • DHCPRELEASE • DHCPINFORM • BOOTPREQUEST
BOOTP Reply	The number of DHCP replies sent from the DHCP server to DHCP clients, including: • DHCPOFFER • DHCPACK • DHCPNAK • BOOTPREPLY
Bad Messages	The number of erroneous messages

display dhcp server tree

Syntax

display dhcp server tree { **all** | **pool** [*pool-name*] } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

all: Displays information of all DHCP address pools.

pool [*pool-name*]: Displays information of a specified address pool. The *pool name* argument is a string of 1 to 35 characters. If no *pool name* is specified, information of all address pools will be displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display dhcp server tree** command to display information of DHCP address pool(s).

Examples

Display information of all DHCP address pools.

```
<Sysname> display dhcp server tree all
Global pool:

Pool name: 0
 network 20.1.1.0 mask 255.255.255.0
 Sibling node:1
 option 2 ip-address 1.1.1.1
 expired 1 0 0

Pool name: 1
 static-bind ip-address 10.10.1.2 mask 255.0.0.0
 static-bind mac-address 00e0-00fc-0001
 PrevSibling node:0
 expired unlimited

Extended pool:

Pool name: 2
 network ip range 1.1.1.0 1.1.1.255
 network mask 255.255.255.0
 expired 0 0 2
```

Table 9 Output description

Field	Description
Global pool	Information of a common address pool
Pool name	Address pool name
network	Network segment for address allocation

Field	Description
static-bind ip-address 10.10.1.2 mask 255.0.0.0 static-bind mac-address 00e0-00fc-0001	The IP address and MAC address of the static binding
Sibling node	The sibling node of the current node, nodes of this kind in the output information include: • Child node: The child node (subnet segment) address pool of the current node • Parent node: The parent node (nature network segment) address pool of the current node • Sibling node: The latter sibling node of the current node (another subnet of the same nature network). The earlier the sibling node is configured, the higher order the sibling node has. • PrevSibling node: The previous sibling node of the current node
option	Self-defined DHCP options
expired	The lease duration, in the format of day, hour, and minute
Extended pool	Information of an extended address pool
network ip range	Range of assignable IP addresses in the extended address pool
network mask	Mask of IP addresses assigned from the extended address pool

dns-list

Syntax

dns-list *ip-address*&<1-8>

undo dns-list { *ip-address* | **all** }

View

DHCP address pool view

Default level

2: System level

Parameters

ip-address&<1-8>: DNS server IP address. &<1-8> means you can specify up to eight DNS server addresses separated by spaces.

all: Specifies all DNS server addresses to be removed.

Description

Use the **dns-list** command to specify DNS server addresses in a DHCP address pool.

Use the **undo dns-list** command to remove DNS server addresses from a DHCP address pool.

By default, no DNS server address is specified.

If you repeatedly use the **dns-list** command, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool** and **display dhcp server tree**.

Examples

Specify the DNS server address 10.1.1.254 for the DHCP client in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] dns-list 10.1.1.254
```

domain-name

Syntax

domain-name *domain-name*

undo domain-name

View

DHCP address pool view

Default level

2: System level

Parameters

domain-name: Domain name suffix for DHCP clients, a string of 1 to 50 characters.

Description

Use the **domain-name** command to specify a domain name suffix for the DHCP clients in the DHCP address pool.

Use the **undo domain-name** command to remove the specified domain name suffix.

No domain name suffix is specified by default.

Related commands: **dhcp server ip-pool** and **display dhcp server tree**.

Examples

Specify a domain name suffix of mydomain.com for the DHCP clients in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] domain-name mydomain.com
```

expired

Syntax

expired { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }

undo expired

View

DHCP address pool view

Default level

2: System level

Parameters

day *day*: Specifies the number of days, in the range of 0 to 365.

hour *hour*: Specifies the number of hours, in the range of 0 to 23.

minute *minute*: Specifies the number of minutes, in the range of 0 to 59.

unlimited: Specifies the unlimited lease duration, which is actually 136 years.

Description

Use the **expired** command to specify the lease duration in a DHCP address pool.

Use the **undo expired** command to restore the default lease duration in a DHCP address pool.

By default, the lease duration of a static binding is unlimited, and the address lease duration in a DHCP address pool configured for dynamic allocation is one day.

Related commands: **dhcp server ip-pool** and **display dhcp server tree**.

Examples

Specify the lease duration as one day, two hours, and three minutes in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] expired day 1 hour 2 minute 3
```

forbidden-ip

Syntax

forbidden-ip *ip-address*&<1-8>

undo forbidden-ip { *ip-address*&<1-8> | **all** }

View

DHCP address pool view

Default level

2: System level

Parameters

ip-address&<1-8>: IP addresses to be excluded from dynamic allocation. &<1-8> indicates that you can specify up to eight IP addresses, separated with spaces.

all: Excludes all IP addresses from dynamic allocation.

Description

Use the **forbidden-ip** command to exclude IP addresses from dynamic allocation in an extended address pool.

Use the **undo forbidden-ip** command to cancel specified or all excluded IP addresses.

By default, all IP addresses in an extended address pool are assignable except the IP addresses of the DHCP server interfaces.

NOTE:

- Only the extended address pools support this command.
- IP addresses specified with the **forbidden-ip** command in DHCP address pool view are excluded from dynamic address allocation in the current extended address pool only. They are assignable in other address pools.
- Repeatedly using the **forbidden-ip** command can exclude multiple IP address ranges from dynamic allocation.

Related commands: **dhcp server ip-pool** and **display dhcp server forbidden-ip**.

Examples

Exclude IP addresses 192.168.1.3 and 192.168.1.10 from dynamic allocation for extended address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0 extended
[Sysname-dhcp-pool-0] forbidden-ip 192.168.1.3 192.168.1.10
```

gateway-list

Syntax

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

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

View

DHCP address pool view

Default level

2: System level

Parameters

ip-address&<1-8>: Gateway IP address. &<1-8> means you can specify up to eight gateway addresses separated by spaces.

all: Specifies all gateway IP addresses to be removed.

Description

Use the **gateway-list** command to specify gateway address(es) in a DHCP address pool.

Use the **undo gateway-list** command to remove specified gateway address(es) specified for the DHCP client from a DHCP address pool.

By default, no gateway address is specified.

If you use the **gateway-list** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool** and **display dhcp server tree**.

Examples

Specify the gateway address 10.110.1.99 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] gateway-list 10.110.1.99
```

nbns-list

Syntax

nbns-list *ip-address*&<1-8>

undo nbns-list { *ip-address* | **all** }

View

DHCP address pool view

Default level

2: System level

Parameters

ip-address&<1-8>: WINS server IP address. &<1-8> means you can specify up to eight WINS server addresses separated by spaces.

all: Specifies all WINS server addresses to be removed.

Description

Use the **nbns-list** command to specify WINS server address(es) in a DHCP address pool.

Use the **undo nbns-list** command to remove the specified WINS server address(es).

By default, no WINS server address is specified.

If you use the **nbns-list** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool**, **netbios-type**, and **display dhcp server tree**.

Examples

Specify WINS server address 10.12.1.99 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] nbns-list 10.12.1.99
```

netbios-type

Syntax

netbios-type { **b-node** | **h-node** | **m-node** | **p-node** }

undo netbios-type

View

DHCP address pool view

Default level

2: System level

Parameters

b-node: Broadcast node. A b-node client sends the destination name in a broadcast message. The destination returns the name-to-IP mapping to the client after receiving the message.

p-node: Peer-to-peer node. A p-node client sends the destination name in a unicast message to the WINS server, and the WINS server returns the mapping to the client.

m-node: Mixed node, a combination of a b-node first and p-node second. An m-node client broadcasts the destination name, if there is no response, and then unicasts the destination name to the WINS server to get the mapping.

h-node: Hybrid node, a combination of a p-node first and b-node second. An h-node is a b-node with the peer-to-peer communication mechanism. An h-node client unicasts the destination name to the WINS server, if there is no response, and then broadcasts it to get the mapping from the destination.

Description

Use the **netbios-type** command to specify the client NetBIOS node type in a DHCP address pool.

Use the **undo netbios-type** command to remove the specified client NetBIOS node type.

By default, no NetBIOS node type is specified.

Related commands: **dhcp server ip-pool**, **nbns-list**, and **display dhcp server tree**.

Examples

Specify the NetBIOS node type as b-node in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] netbios-type b-node
```

network

Syntax

network *network-address* [*mask-length* | **mask** *mask*]

undo network

View

DHCP address pool view

Default level

2: System level

Parameters

network-address: IP address range for dynamic allocation. If no mask length and mask is specified, the natural mask will be used.

mask-length: Mask length, in the range of 1 to 30.

mask *mask*: Specifies the IP address network mask, in dotted decimal format.

Description

Use the **network** command to specify the IP address range for dynamic allocation in a DHCP address pool.

Use the **undo network** command to remove the specified address range.

No IP address range is specified by default.

You can specify only one network segment for each common address pool. If you use the **network** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool** and **display dhcp server tree**.

Examples

Specify 192.168.8.0/24 as the address range for dynamic allocation in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] network 192.168.8.0 mask 255.255.255.0
```

network ip range

Syntax

network ip range *min-address max-address*

undo network ip range

View

DHCP address pool view

Default level

2: System level

Parameters

min-address: Lowest IP address for dynamic allocation.

max-address: Highest IP address for dynamic allocation.

Description

Use the **network ip range** command to specify the IP address range for dynamic allocation in an extended address pool.

Use the **undo network ip range** command to remove the specified address range.

No IP address range is specified by default.

NOTE:

- Only the extended address pools support this command.
- You can specify only one IP address range for each extended address pool. If you use the **network ip range** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool** and **display dhcp server tree**.

Examples

Specify 192.168.8.1 through 192.168.8.150 as the address range for dynamic allocation in extended address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0 extended
[Sysname-dhcp-pool-0] network ip range 192.168.8.1 192.168.8.150
```

network mask

Syntax

network mask *mask*

undo network mask

View

DHCP address pool view

Default level

2: System level

Parameters

mask: Network mask, in dotted decimal notation.

Description

Use the **network mask** command to specify the IP address mask for dynamic allocation in an extended address pool.

Use the **undo network mask** command to remove the specified IP address mask.

No IP address mask is specified by default.

NOTE:

- Only the extended address pools support this command.
- If you specify an IP address range for an extended address pool without an IP address mask, the extended address pool is not valid, and therefore the system cannot assign IP addresses from the extended address pool.

Related commands: **dhcp server ip-pool**, **network ip range**, and **display dhcp server tree**.

Examples

Specify 255.255.255.0 as the IP address mask for dynamic allocation in extended address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0 extended
[Sysname-dhcp-pool-0] network mask 255.255.255.0
```

option

Syntax

option *code* { **ascii** *ascii-string* | **hex** *hex-string*&<1-16> | **ip-address** *ip-address*&<1-8> }

undo option *code*

View

DHCP address pool view

Default level

2: System level

Parameters

code: Self-defined option number, in the range of 2 to 254, excluding 12, 50 to 55, 57 to 61, and 82.

ascii *ascii-string*: Specifies an ASCII string with 1 to 255 characters.

hex *hex-string*&<1-16>: Specifies hex digit strings. &<1-16> indicates that you can specify up to 16 hex digit strings, separated by spaces. Each string contains 2, 4, 6 or 8 hex digits.

ip-address *ip-address*&<1-8>: Specifies IP addresses. &<1-8> indicates that you can specify up to eight IP addresses, separated by spaces.

Description

Use the **option** command to configure a self-defined DHCP option in a DHCP address pool.

Use the **undo option** command to remove a self-defined DHCP option from a DHCP address pool.

The **option** command is not configured by default.

If you use the **option** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool** and **display dhcp server tree**.

Examples

Configure the hex digits 0x11 and 0x22 for the self-defined DHCP Option 100 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] option 100 hex 11 22
```

reset dhcp server conflict

Syntax

reset dhcp server conflict { **all** | **ip** *ip-address* }

View

User view

Default level

2: System level

Parameters

all: Clears the statistics of all IP address conflicts.

ip *ip-address*: Clears the conflict statistics of a specified IP address.

Description

Use the **reset dhcp server conflict** command to clear statistics of IP address conflict(s).

Related commands: **display dhcp server conflict**.

Examples

Clears the statistics of all IP address conflicts.

```
<Sysname> reset dhcp server conflict all
```

reset dhcp server ip-in-use

Syntax

reset dhcp server ip-in-use { **all** | **ip** *ip-address* | **pool** [*pool-name*] }

View

User view

Default level

2: System level

Parameters

all: Clears the IP address dynamic binding information of all DHCP address pools.

ip *ip-address*: Clears the dynamic binding information of a specified IP address.

pool [*pool-name*]: Clears the dynamic binding information of a specified address pool. The *pool name* is a string of 1 to 35 characters. If no *pool name* is specified, the dynamic binding information of all address pools is cleared.

Description

Use the **reset dhcp server ip-in-use** command to clear dynamic IP address binding information.

Related commands: **display dhcp server ip-in-use**.

Examples

Clear the binding information of IP address 10.110.1.1.

```
<Sysname> reset dhcp server ip-in-use ip 10.110.1.1
```

reset dhcp server statistics

Syntax

reset dhcp server statistics

View

User view

Default level

2: System level

Parameters

None

Description

Use the **reset dhcp server statistics** command to clear the statistics of the DHCP server.

Related commands: **display dhcp server statistics**.

Examples

Clear the statistics of the DHCP server.

```
<Sysname> reset dhcp server statistics
```

static-bind client-identifier

Syntax

static-bind client-identifier *client-identifier*

undo static-bind client-identifier

View

DHCP address pool view

Default level

2: System level

Parameters

client-identifier: The client ID of a static binding, a string with 4 to 160 characters in the format of H-H-H…, each H indicates 4 hex digits except the last H indicates 2 or 4 hex digits. For example, aabb-cccc-dd is a valid ID, but aabb-c-dddd and aabb-cc-dddd are both invalid.

Description

Use the **static-bind client-identifier** command to specify the client ID of a static binding in a DHCP address pool.

Use the **undo static-bind client-identifier** command to remove the client ID of a static binding from a DHCP address pool.

By default, no client ID is specified.

- Use the **static-bind client-identifier** command together with the **static-bind ip-address** command to accomplish a static binding configuration.
- The ID of the static binding of a client must be identical to the ID displayed by using the **display dhcp client verbose** command on the client. Otherwise, the client cannot obtain an IP address.
- If you use the **static-bind client-identifier** or **static-bind mac-address** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool**, **static-bind ip-address**, **static-bind mac-address**, **display dhcp server tree**, and **display dhcp client verbose**.

Examples

Bind the client ID aaaa-bbbb to the IP address 10.1.1.1 with the mask 255.255.255.0 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
[Sysname-dhcp-pool-0] static-bind client-identifier aaaa-bbbb
```

static-bind ip-address

Syntax

static-bind ip-address *ip-address* [*mask-length* | **mask** *mask*]

undo static-bind ip-address

View

DHCP address pool view

Default level

2: System level

Parameters

ip-address: IP address of a static binding. If no mask and mask length is specified, the natural mask is used.

mask-length: Mask length of the IP address, which is the number of 1s in the mask, in the range of 0 to 32.

mask *mask*: Specifies the IP address mask, in dotted decimal format.

Description

Use the **static-bind ip-address** command to specify an IP address in a DHCP address pool for a static binding.

Use the **undo static-bind ip-address** command to remove the statically bound IP address.

By default, no IP address is statically bound in a DHCP address pool.

- Use the **static-bind ip-address** command together with the **static-bind mac-address** or **static-bind client-identifier** command to accomplish a static binding configuration.
- The IP address of the static binding cannot be an interface address of the DHCP server. Otherwise, an IP address conflict may occur, and the bound client cannot obtain an IP address correctly.
- If you use the **static-bind ip-address** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool**, **static-bind client-identifier**, **static-bind mac-address**, and **display dhcp server tree**.

Examples

Bind the client MAC address 0000-e03f-0305 to the IP address 10.1.1.1 with the mask 255.255.255.0 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
[Sysname-dhcp-pool-0] static-bind mac-address 0000-e03f-0305
```

static-bind mac-address

Syntax

static-bind mac-address *mac-address*

undo static-bind mac-address

View

DHCP address pool view

Default level

2: System level

Parameters

mac-address: The MAC address of a static binding, in the format of H-H-H.

Description

Use the **static-bind mac-address** command to statically bind a MAC address to an IP address in a DHCP address pool.

Use the **undo static-bind mac-address** command to remove the statically bound MAC address.

By default, no MAC address is statically bound.

- Use the **static-bind mac-address** command together with the **static-bind ip-address** command to complete a static binding configuration.
- If you use the **static-bind mac-address** or **static-bind client-identifier** command repeatedly, the latest configuration will overwrite the previous one.

Relate commands: **dhcp server ip-pool**, **static-bind client-identifier**, **static-bind ip-address**, **display dhcp server tree**.

Examples

Bind the client MAC address 0000-e03f-0305 to the IP address 10.1.1.1 with the mask 255.255.255.0 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
[Sysname-dhcp-pool-0] static-bind mac-address 0000-e03f-0305
```

tftp-server domain-name

Syntax

tftp-server domain-name *domain-name*

undo tftp-server domain-name

View

DHCP address pool view

Default level

2: System level

Parameters

domain-name: TFTP server name, a string of 1 to 63 characters.

Description

Use the **tftp-server domain-name** command to specify a TFTP server name in a DHCP address pool.

Use the **undo tftp-server domain-name** command to remove the TFTP server name from a DHCP address pool.

By default, no TFTP server name is specified.

Using the **tftp-server domain-name** command repeatedly will overwrite the previous configuration.

Related commands: **dhcp server ip-pool** and **display dhcp server tree**.

Examples

Specify the TFTP server name as **aaa** in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] tftp-server domain-name aaa
```

tftp-server ip-address

Syntax

tftp-server ip-address *ip-address*

undo tftp-server ip-address

View

DHCP address pool view

Default level

2: System level

Parameters

ip-address: TFTP server IP address.

Description

Use the **tftp-server ip-address** command to specify the TFTP server IP address in a DHCP address pool.

Use the **undo tftp-server ip-address** command to remove the TFTP server IP address from a DHCP address pool.

By default, no TFTP server address is specified.

Using the **tftp-server ip-address** command repeatedly will overwrite the previous configuration.

Related commands: **dhcp server ip-pool** and **display dhcp server tree**.

Examples

Specify the TFTP server address 10.1.1.1 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] tftp-server ip-address 10.1.1.1
```

vendor-class-identifier

Syntax

vendor-class-identifier *hex-string*&<1-255> **ip range** *min-address max-address*

undo vendor-class-identifier *hex-string*&<1-255>

View

DHCP extended address pool view

Default level

2: System level

Parameters

hex-string&<1-255>: A character string, which is used to match against Option 60 (vendor class identifier option). *hex-string* is a hexadecimal number ranging from 0 to FF. &<1-255> indicates that you can type up to 255 hexadecimal numbers, which are separated by spaces.

ip range *min-address max-address*: Specifies the IP address range for dynamic allocation. *min-address* is the lowest IP address and *max-address* is the highest IP address for dynamic allocation.

Description

Use the **vendor-class-identifier** command to specify an IP address range for the DHCP clients of a specified vendor.

Use the **undo vendor-class-identifier** command to restore the default.

By default, no IP address range is specified for the DHCP clients of any vendor.

After this feature is configured in an extended DHCP address pool, the DHCP server, when using the extended DHCP address pool to assign an IP address to a DHCP client, checks whether Option 60 in the DHCP request is the same as the character string configured with the **vendor-class-identifier** command. If yes, the DHCP server selects an IP address from the address range specified with this command. If not, the DHCP server selects one from the address range specified with the **network ip range** command.

NOTE:

- Only extended address pools support this command.
- The IP address range specified with this command must be included in that specified with the **network ip range** command.

Related commands: **network ip range** and **network mask**.

Examples

Specify IP address 10.1.1.1 to 10.1.1.5 for the DHCP clients of vender a0 b0 0c.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0 extended
[Sysname-dhcp-pool-0] vendor-class-identifier a0 b0 0c ip range 10.1.1.1 10.1.1.5
```

voice-config

Syntax

voice-config { **as-ip** *ip-address* | **fail-over** *ip-address dialer-string* | **ncp-ip** *ip-address* | **voice-vlan** *vlan-id* { **disable** | **enable** } }

undo voice-config [**as-ip** | **fail-over** | **ncp-ip** | **voice-vlan**]

View

DHCP address pool view

Default level

2: System level

Parameters

as-ip *ip-address*: Specifies the IP address for the backup network calling processor. When the primary network calling processor is unavailable, the DHCP client uses the backup network calling processor.

fail-over *ip-address dialer-string*: Specifies the failover IP address and dialer string. The *dialer-string* is a string of 1 to 39 characters, which can be 0 to 9, and "*".

ncp-ip *ip-address*: Specifies the IP address for the primary network calling processor.

voice-vlan *vlan-id*: Specifies the voice VLAN ID, in the range of 2 to 4094.

- **disable**: Disables the specified voice VLAN ID, meaning DHCP clients will not take this ID as their voice VLAN.
- **enable**: Enables the specified voice VLAN ID, meaning DHCP clients will take this ID as their voice VLAN.

Description

Use the **voice-config** command to configure specified Option 184 contents in a DHCP address pool.

Use the **undo voice-config** command to remove specified Option 184 contents from a DHCP address pool.

By default, no Option 184 content is configured.

Note that specifying the IP address of a network calling processor first is necessary to make other configured parameters take effect.

Related commands: **dhcp server ip-pool**, and **display dhcp server tree**.

Examples

Configure Option 184 in DHCP address pool 0: the primary network calling processor 10.1.1.1, backup network calling processor 10.2.2.2, voice VLAN ID 3 that is enabled, the failover IP address 10.3.3.3 and dialer string 99*.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] voice-config ncp-ip 10.1.1.1
```

```
[Sysname-dhcp-pool-0] voice-config as-ip 10.2.2.2
[Sysname-dhcp-pool-0] voice-config voice-vlan 3 enable
[Sysname-dhcp-pool-0] voice-config fail-over 10.3.3.3 99*
```

DHCP relay agent configuration commands

NOTE:

The DHCP relay agent configuration is supported only on VLAN interfaces.

dhcp relay address-check

Syntax

dhcp relay address-check { **disable** | **enable** }

View

Interface view

Default level

2: System level

Parameters

disable: Disables address check on the relay agent.

enable: Enables address check on the relay agent.

Description

Use the **dhcp relay address-check enable** command to enable address check on the relay agent.

Use the **dhcp relay address-check disable** command to disable address check on the relay agent.

By default, the function is disabled.

With this feature enabled, the DHCP relay agent can dynamically record clients' IP-to-MAC bindings after clients get IP addresses through DHCP. It also supports static bindings. you can manually configure IP-to-MAC bindings on the DHCP relay agent, so that users can access external networks using fixed IP addresses.

Upon receiving an ARP packet, the DHCP relay agent matches the sender's IP and MAC addresses in the packet against the bindings (both dynamic and static). If no match is found, the DHCP relay agent does not learn the ARP entry. The sending host cannot access external networks via the DHCP relay agent.

The **dhcp relay address-check enable** command only checks IP and MAC addresses of clients.

Examples

Enable address check on the DHCP relay agent.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay address-check enable
```

dhcp relay check mac-address

Syntax

dhcp relay check mac-address

undo dhcp relay check mac-address

View

Interface view

Default level

2: System level

Parameters

None

Description

Use the **dhcp relay check mac-address** command to enable MAC address check on the DHCP relay agent.

Use the **undo dhcp relay check mac-address** command to disable MAC address check on the DHCP relay agent.

By default, this function is disabled.

With this function enabled, the DHCP relay agent compares the chaddr field of a received DHCP request with the source MAC address field of the frame. If they are the same, the DHCP relay agent decides this request as valid and forwards it to the DHCP server; if not, the DHCP request is discarded.

Note that DHCP relay agents change the source MAC addresses when forwarding DHCP packets. Therefore, you can enable MAC address check only on a DHCP relay agent directly connected to the DHCP clients. Otherwise, valid DHCP packets may be discarded and clients cannot obtain IP addresses.

Examples

Enable MAC address check on the DHCP relay agent.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay check mac-address
```

dhcp relay client-detect enable

Syntax

dhcp relay client-detect enable

undo dhcp relay client-detect enable

View

Interface view

Default level

2: System level

Parameters

None

Description

Use the **dhcp relay client-detect enable** command to enable offline detection on the DHCP relay agent.

Use the **undo dhcp relay client-detect enable** command to disable offline detection on the DHCP relay agent.

By default, this function is disabled.

With this function enabled on an interface, the DHCP relay agent removes a client's IP-to-MAC binding entry when it is aged out, and sends a DHCP-RELEASE request to the DHCP server to release the IP address of the client.

Examples

Enable offline detection on the DHCP relay agent.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay client-detect enable
```

dhcp relay information circuit-id format-type

Syntax

dhcp relay information circuit-id format-type { **ascii** | **hex** }

undo dhcp relay information circuit-id format-type

View

Interface view

Default level

2: System level

Parameters

ascii: Specifies the code type for the circuit ID sub-option as **ascii**.

hex: Specifies the code type for the circuit ID sub-option as **hex**.

Description

Use the **dhcp relay information circuit-id format-type** command to configure the code type for the non-user-defined circuit ID sub-option.

Use the **undo dhcp relay information circuit-id format-type** command to restore the default.

By default, the code type for the circuit ID sub-option depends on the specified padding format of Option 82. Each field has its own code type.

This command applies to configuring the non-user-defined circuit ID sub-option only. After you configure the padding content for the circuit ID sub-option using the **dhcp relay information circuit-id string** command, ASCII is adopted as the code type.

Related commands: **display dhcp relay information**.

Examples

Configure the code type for the non-user-defined circuit ID sub-option as **ascii**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information circuit-id format-type ascii
```

dhcp relay information circuit-id string

Syntax

dhcp relay information circuit-id string *circuit-id*

undo dhcp relay information circuit-id string

View

Interface view

Default level

2: System level

Parameters

circuit-id: Padding content for the user-defined circuit ID sub-option, a case-sensitive string of 3 to 63 characters.

Description

Use the **dhcp relay information circuit-id string** command to configure the padding content for the user-defined circuit ID sub-option.

Use the **undo dhcp relay information circuit-id string** command to restore the default.

By default, the padding content for the circuit ID sub-option depends on the padding format of Option 82.

After you configure the padding content for the circuit ID sub-option using this command, ASCII is adopted as the code type.

Related commands: **dhcp relay information format** and **display dhcp relay information**.

Examples

Configure the padding content for the circuit ID sub-option as **company001**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information circuit-id string company001
```

dhcp relay information enable

Syntax

dhcp relay information enable

undo dhcp relay information enable

View

Interface view

Default level

2: System level

Parameters

None

Description

Use the **dhcp relay information enable** command to enable the relay agent to support Option 82.

Use the **undo dhcp relay information enable** command to disable Option 82 support.

By default, Option 82 support is disabled on DHCP relay agent.

Related commands: **display dhcp relay information**.

Examples

Enable Option 82 support on the relay agent.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information enable
```

dhcp relay information format

Syntax

dhcp relay information format { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] }

undo dhcp relay information format [**verbose node-identifier**]

View

Interface view

Default level

2: System level

Parameters

normal: Specifies the normal padding format.

verbose: Specifies the verbose padding format.

node-identifier { **mac** | **sysname** | **user-defined** *node-identifier* }: Specifies access node identifier. By default, the node MAC address is used as the node identifier.

- **mac** indicates using MAC address as the node identifier.
- **sysname** indicates using the device name of a node as the node identifier.
- **user-defined** *node-identifier* indicates using a specified character string as the node identifier, in which *node-identifier* is a string with 1 to 50 characters.

Description

Use the **dhcp relay information format** command to specify a padding format for Option 82.

Use the **undo dhcp relay information format** command to restore the default padding format.

The Option 82 padding format defaults to **normal**.

NOTE:

- Using the **undo dhcp relay information format** command without the keyword **verbose node-identifier** restores the default **normal** padding format, or with the keyword **verbose node-identifier** restores the **mac** mode of the **verbose** padding format.
- If configuring the handling strategy of the DHCP relay agent as **replace**, you need to configure a padding format of Option 82. If the handling strategy is **keep** or **drop**, you need not configure any padding format.
- If sub-option 1 (node identifier) of Option 82 is padded with the device name (sysname) of a node, the device name must contain no spaces. Otherwise, the DHCP relay agent will drop the message.

Related commands: **display dhcp relay information**.

Examples

Specify the verbose padding format for Option 82.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information enable
[Sysname-Vlan-interface1] dhcp relay information strategy replace
[Sysname-Vlan-interface1] dhcp relay information format verbose
```

dhcp relay information remote-id format-type

Syntax

dhcp relay information remote-id format-type { **ascii** | **hex** }

undo dhcp relay information remote-id format-type

View

Interface view

Default level

2: System view

Parameters

ascii: Specifies the code type for the remote ID sub-option as **ascii**.

hex: Specifies the code type for the remote ID sub-option as **hex**.

Description

Use the **dhcp relay information remote-id format-type** command to configure the code type for the non-user-defined remote ID sub-option.

Use the **undo dhcp relay information remote-id format-type** command to restore the default.

By default, the code type for the remote ID sub-option is HEX.

This command applies to configuring the non-user-defined remote ID sub-option only. After you configure the padding content for the remote ID sub-option using the **dhcp relay information remote-id string** command, ASCII is adopted as the code type.

Related commands: **display dhcp relay information**.

Examples

Configure the code type for the non-user-defined remote ID sub-option as **ascii**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information remote-id format-type ascii
```

dhcp relay information remote-id string

Syntax

dhcp relay information remote-id string { *remote-id* | **sysname** }

undo dhcp relay information remote-id string

View

Interface view

Default level

2: System level

Parameters

remote-id: Padding content for the user-defined remote ID sub-option, a case sensitive string of 1 to 63 characters.

sysname: Specifies the device name as the padding content for the remote ID sub-option.

Description

Use the **dhcp relay information remote-id string** command to configure the padding content for the user-defined remote ID sub-option.

Use the **undo dhcp relay information remote-id string** command to restore the default.

By default, the padding content for the remote ID sub-option depends on the padding format of Option 82.

After you configure the padding content for the remote ID sub-option using this command, ASCII is adopted as the code type.

NOTE:

If you want to specify the character string **sysname** (a case-insensitive character string) as the padding content for the remote ID sub-option, you need to use quotation marks to make it take effect. For example, if you want to specify **Sysname** as the padding content for the remote ID sub-option, you need to enter the **dhcp relay information remote-id string** "Sysname" command.

Related commands: **dhcp relay information format** and **display dhcp relay information**.

Examples

Configure the padding content for the remote ID sub-option as **device001**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information remote-id string device001
```

dhcp relay information strategy

Syntax

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

undo dhcp relay information strategy

View

Interface view

Default level

2: System level

Parameters

drop: Specifies to drop messages containing Option 82.

keep: Specifies to forward messages containing Option 82 without any change.

replace: Specifies to forward messages containing Option 82 after replacing the original Option 82 with the Option 82 padded in the specified padding format.

Description

Use the **dhcp relay information strategy** command to configure DHCP relay agent handling strategy for messages containing Option 82.

Use the **undo dhcp relay information strategy** command to restore the default handling strategy.

The handling strategy for messages containing Option 82 defaults to **replace**.

Related commands: **display dhcp relay information**.

Examples

Configure the DHCP relay agent handling strategy for messages containing Option 82 as **keep**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information enable
[Sysname-Vlan-interface1] dhcp relay information strategy keep
```

dhcp relay release ip

Syntax

dhcp relay release ip *client-ip*

View

System view

Default level

2: System level

Parameters

client-ip: DHCP client IP address.

Description

Use the **dhcp relay release ip** command to request the DHCP server to release a specified client IP address.

Examples

Request the DHCP server to release the IP address 1.1.1.1.

```
<Sysname> system-view
[Sysname] dhcp relay release ip 1.1.1.1
```

dhcp relay security static

Syntax

dhcp relay security static *ip-address mac-address* [**interface** *interface-type interface-number*]

undo dhcp relay security { *ip-address* | **all** | **dynamic** | **interface** *interface-type interface-number* | **static** }

View

System view

Default level

2: System level

Parameters

ip-address: Client IP address for creating a static binding.

mac-address: Client MAC address for creating a static binding, in the format H-H-H.

interface *interface-type interface-number*: Specifies a Layer 3 interface connecting to the DHCP client. *interface-type interface-number* specifies the interface type and interface number.

all: Specifies all client entries to be removed.

dynamic: Specifies dynamic client entries to be removed.

static: Specifies manual client entries to be removed.

Description

Use the **dhcp relay security static** command to configure a static client entry, which is the binding between IP address, MAC address, and Layer 3 interface on the relay agent.

Use the **undo dhcp relay security** command to remove specified client entries from the relay agent.

No manual client entry is configured on the DHCP relay agent by default.

- When using the **dhcp relay security static** command to bind an interface to a static client entry, make sure that the interface is configured as a DHCP relay agent; otherwise, entry conflicts may occur.
- The **undo dhcp relay security interface** command is used to remove all the dynamic client entries from the interface.

Related commands: **display dhcp relay security**.

Examples

Bind DHCP relay interface VLAN-interface 2 to IP address 10.10.1.1 and MAC address 0005-5d02-f2b3 of the client.

```
<Sysname> system-view
[Sysname] dhcp relay security static 10.10.1.1 0005-5d02-f2b3 interface vlan-interface
2
```

dhcp relay security refresh enable

Syntax

dhcp relay security refresh enable

undo dhcp relay security refresh enable

View

System view

Default level

2: System level

Parameters

None

Description

Use the **dhcp relay security refresh enable** command to enable the DHCP relay agent to periodically refresh dynamic client entries.

Use the **undo dhcp relay security refresh enable** command to disable periodic refresh of dynamic client entries.

By default, the DHCP relay agent is enabled to periodically refresh dynamic client entries.

If you disable the DHCP relay agent from periodically refreshing dynamic client entries, such entries do not age automatically. Therefore, if a client relinquishes its IP address, you need to manually remove the corresponding dynamic client entry on the DHCP relay agent.

Related commands: **dhcp relay security tracker** and **dhcp relay security static**.

Examples

Disable the DHCP relay agent from periodically refreshing dynamic client entries.

```
<Sysname> system-view
[Sysname] undo dhcp relay security refresh enable
```

dhcp relay security tracker

Syntax

dhcp relay security tracker { *interval* | **auto** }

undo dhcp relay security tracker [*interval*]

View

System view

Default level

2: System level

Parameters

interval: Refreshing interval in seconds, in the range of 1 to 120.

auto: Specifies the **auto** refreshing interval, which is the value of 60 seconds divided by the number of binding entries. Thus, the more entries are, the shorter interval is, but the shortest interval is no less than 500 ms.

Description

Use the **dhcp relay security tracker** command to set a refreshing interval at which the relay agent contacts the DHCP server for refreshing dynamic bindings.

Use the **undo dhcp relay security tracker** command to restore the default interval.

The default refreshing interval is **auto**, the value of 60 seconds divided by the number of binding entries.

Related commands: **display dhcp relay security tracker**.

Examples

Set the refreshing interval as 100 seconds.

```
<Sysname> system-view
[Sysname] dhcp relay security tracker 100
```

dhcp relay server-detect

Syntax

dhcp relay server-detect

undo dhcp relay server-detect

View

System view

Default level

2: System level

Parameters

None

Description

Use the **dhcp relay server-detect** command to enable unauthorized DHCP server detection.

Use the **undo dhcp relay server-detect** command to disable unauthorized DHCP server detection.

By default, unauthorized DHCP server detection is disabled.

With this function enabled, upon receiving a DHCP request, the DHCP relay agent will resolve from the request the IP addresses of all DHCP servers which ever offered IP addresses to the DHCP client and the receiving interface. Each server detected is recorded only once. The administrator can get this information from logs to check out unauthorized DHCP servers.

After the information of recorded DHCP servers is cleared, the relay agent will re-record server information following this mechanism.

Examples

Enable unauthorized DHCP server detection.

```
<Sysname> system-view
[Sysname] dhcp relay server-detect
```

dhcp relay server-group

Syntax

dhcp relay server-group *group-id* **ip** *ip-address*

undo dhcp relay server-group *group-id* [**ip** *ip-address*]

View

System view

Default level

2: System level

Parameters

group-id: DHCP server group number, in the range of 0 to 19.

ip *ip-address*: DHCP server IP address.

Description

Use the **dhcp relay server-group** command to specify a DHCP server for a DHCP server group.

Use the **undo dhcp relay server-group** command to remove a DHCP server from a DHCP server group, if no **ip** *ip-address* is specified, all servers in the DHCP server group and the server group itself will be removed.

By default, no DHCP server is specified for a DHCP server group.

The IP addresses of any DHCP server and DHCP relay agent's interface that connects the DHCP client cannot be in the same network segment. Otherwise, the client may fail to obtain an IP address.

If a server group has been correlated to multiple interfaces, you need to cancel these correlations before removing the server group.

Related commands: **display dhcp relay server-group**.

Examples

Specify DHCP server 1.1.1.1 for DHCP server group 1 on the relay agent.

```
<Sysname> system-view
[Sysname] dhcp relay server-group 1 ip 1.1.1.1
```

dhcp relay server-select

Syntax

dhcp relay server-select *group-id*

undo dhcp relay server-select

View

Interface view

Default level

2: System level

Parameters

group-id: DHCP server group number to be correlated, in the range of 0 to 19.

Description

Use the **dhcp relay server-select** command to correlate specified interface(s) to a specified DHCP server group.

Use the **undo dhcp relay server-select** command to remove a configured correlation.

By default, no DHCP server group is correlated with an interface on the relay agent.

A DHCP server group can correlate with one or multiple DHCP relay agent interfaces.

A relay agent interface can only correlate with one DHCP server group, and a newly configured correlation overwrites the previous one. If the server group in the new correlation does not exist, the new configuration will not work. The interface still maintains the previous correlation.

The DHCP server group referenced in this command should have been configured by using the **dhcp relay server-group** command.

Related commands: **dhcp relay server-group** and **display dhcp relay**.

Examples

Correlate VLAN-interface 1 to DHCP server group 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
```

```
[Sysname-Vlan-interface1] dhcp relay server-select 1
```

dhcp select relay

Syntax

dhcp select relay

undo dhcp select relay

View

Interface view

Default level

2: System level

Parameters

None

Description

Use the **dhcp select relay** command to enable the relay agent on the current interface. Upon receiving requests from an enabled interface, the relay agent will forward these requests to outside DHCP servers for IP address allocation.

Use the **undo dhcp select relay** command to restore the default.

After DHCP is enabled, the DHCP server is enabled on an interface by default. Upon receiving a client's request from the interface, the DHCP server allocates an IP address from the DHCP address pool to the client.

When the working mode of the interface is changed from DHCP server to DHCP relay agent, the IP address leases will not be deleted. However, these ARP entries may conflict with new ARP entries generated on the DHCP relay agent. You can delete the existing IP address leases when changing the interface working mode to DHCP relay agent.

Examples

Enable the DHCP relay agent on VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp select relay
```

display dhcp relay

Syntax

display dhcp relay { **all** | **interface** *interface-type interface-number* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

all: Displays information of DHCP server groups that all interfaces correspond to.

interface *interface-type interface-number*: Displays information of the DHCP server group that a specified interface corresponds to.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display dhcp relay** command to display information about DHCP server groups correlated to an interface or all interfaces.

Examples

Display information about DHCP server groups correlated to all interfaces.

```
<Sysname> display dhcp relay all
    Interface name            Server-group
    Vlan-interface1                  2
```

Table 10 Output description

Field	Description
Server-group	DHCP server group number correlated to the interface.

display dhcp relay information

Syntax

display dhcp relay information { **all** | **interface** *interface-type interface-number* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

all: Displays the Option 82 configuration information of all interfaces.

interface *interface-type interface-number*: Displays the Option 82 configuration information of a specified interface.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display dhcp relay information** command to display Option 82 configuration information on the DHCP relay agent.

Examples

Display the Option 82 configuration information of all interfaces.

```
<Sysname> display dhcp relay information all
Interface: Vlan-interface100
    Status: Enable
    Strategy: Replace
    Format: Verbose
    Circuit ID format-type: HEX
    Remote ID format-type: ASCII
    Node identifier: aabbcc
    User defined:
         Circuit ID: company001
Interface: Vlan-interface200
    Status: Enable
    Strategy: Keep
    Format: Normal
    Circuit ID format-type: HEX
    Remote ID format-type: ASCII
    User defined:
         Remote ID: device001
```

Table 11 Output description

Field	Description
Interface	Interface name
Status	Option 82 state, which can be **Enable** or **Disable**.
Strategy	Handling strategy for requesting messages containing Option 82, which can be **Drop**, **Keep**, or **Replace**.
Format	Padding format of Option 82, which can be **Normal** or **Verbose**.
Circuit ID format-type	Non-user-defined code type of the circuit ID sub-option, which can be **ASCII** or **HEX**.
Remote ID format-type	Non-user-defined code type of the remote ID sub-option, which can be **ASCII** or **HEX**.
Node identifier	Access node identifier
User defined	Content of user-defined sub-options
Circuit ID	User-defined padding content of the circuit ID sub-option
Remote ID	User-defined padding content of the remote ID sub-option

display dhcp relay security

Syntax

display dhcp relay security [*ip-address* | **dynamic** | **static**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

ip-address: Displays the binding information of an IP address.

dynamic: Displays information about dynamic bindings.

static: Displays information about static bindings.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display dhcp relay security** command to display information about bindings of DHCP relay agents. If no parameter is specified, information about all bindings will be displayed.

Note that you need to enable address check, or IP source guard on the DHCP relay agent before it can generate dynamic client entries. For more information about IP source guard, see the *Security Configuration Guide*.

Examples

Display information about all bindings.

```
<Sysname> display dhcp relay security
IP Address      MAC Address     Type       Interface
 10.1.1.1       00e0-0000-0001  Static     vlan1
 10.1.1.5       00e0-0000-0000  Static     Vlan2
---   2 dhcp-security item(s) found   ---
```

Table 12 Output description

Field	Description
IP Address	Client IP address
MAC Address	Client MAC address
Type	Type of binding, including dynamic, static, and temporary.
Interface	Layer 3 interface connecting to the DHCP client. If no interface is recorded in the binding entry, "N/A" is displayed.

display dhcp relay security statistics

Syntax

display dhcp relay security statistics [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display dhcp relay security statistics** command to display statistics information about bindings of DHCP relay agents.

Note that you need to enable address check, or IP source guard on the DHCP relay agent before it can generate dynamic client entries. For more information about IP source guard, see the *Security Configuration Guide*.

Examples

Display statistics about bindings of DHCP relay agents.

```
<Sysname> display dhcp relay security statistics
Static Items      :1
Dynamic Items     :0
Temporary Items   :0
All Items         :1
```

Table 13 Output description

Field	Description
Static Items	Static binding items
Dynamic Items	Dynamic binding items
Temporary Items	Temporary binding items
All Items	All binding items

display dhcp relay security tracker

Syntax

display dhcp relay security tracker [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display dhcp relay security tracker** command to display the interval for refreshing dynamic bindings on the relay agent.

Examples

Display the interval for refreshing dynamic bindings on the relay agent.

```
<Sysname> display dhcp relay security tracker
 Current tracker interval : 10s
```

The interval is 10 seconds.

display dhcp relay server-group

Syntax

display dhcp relay server-group { *group-id* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

group-id: Displays the information of the specified DHCP server group numbered from 0 to 19.

all: Displays the information of all DHCP server groups.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display dhcp relay server-group** command to display the configuration information of a specified or all DHCP server groups.

Examples

Display IP addresses of DHCP servers in DHCP server group 1.

```
<Sysname> display dhcp relay server-group 1
```

```
No.             Group IP
1               1.1.1.1
2               1.1.1.2
```

Table 14 Output description

Field	Description
No.	Sequence number
Group IP	IP address in the server group

display dhcp relay statistics

Syntax

display dhcp relay statistics [**server-group** { *group-id* | **all** }] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

group-id: Specifies a server group number in the range of 0 to 19 about which to display DHCP packet statistics.

all: Specifies all server groups about which to display DHCP packet statistics. Information for each group will be displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display dhcp relay statistics** command to display DHCP packet statistics related to a specified or all DHCP server groups.

Note that if no parameter is specified, all DHCP packet statistics on the relay agent will be displayed.

Related commands: **reset dhcp relay statistics**.

Examples

Display all DHCP packet statistics on the relay agent.

```
<Sysname> display dhcp relay statistics
     Bad packets received:                    0
     DHCP packets received from clients:      0
         DHCPDISCOVER packets received:       0
         DHCPREQUEST packets received:        0
```

```
        DHCPINFORM packets received:         0
        DHCPRELEASE packets received:        0
        DHCPDECLINE packets received:        0
        BOOTPREQUEST packets received:       0
    DHCP packets received from servers:      0
        DHCPOFFER packets received:          0
        DHCPACK packets received:            0
        DHCPNAK packets received:            0
        BOOTPREPLY packets received:         0
    DHCP packets relayed to servers:         0
        DHCPDISCOVER packets relayed:        0
        DHCPREQUEST packets relayed:         0
        DHCPINFORM packets relayed:          0
        DHCPRELEASE packets relayed:         0
        DHCPDECLINE packets relayed:         0
        BOOTPREQUEST packets relayed:        0
    DHCP packets relayed to clients:         0
        DHCPOFFER packets relayed:           0
        DHCPACK packets relayed:             0
        DHCPNAK packets relayed:             0
        BOOTPREPLY packets relayed:          0
    DHCP packets sent to servers:            0
        DHCPDISCOVER packets sent:           0
        DHCPREQUEST packets sent:            0
        DHCPINFORM packets sent:             0
        DHCPRELEASE packets sent:            0
        DHCPDECLINE packets sent:            0
        BOOTPREQUEST packets sent:           0
    DHCP packets sent to clients:            0
        DHCPOFFER packets sent:              0
        DHCPACK packets sent:                0
        DHCPNAK packets sent:                0
        BOOTPREPLY packets sent:             0
```

Display DHCP packet statistics related to every server group on the relay agent.

```
<Sysname> display dhcp relay statistics server-group all
DHCP relay server-group           #0
     Packet type               Packet number
 Client -> Server:
     DHCPDISCOVER                   0
     DHCPREQUEST                    0
     DHCPINFORM                     0
     DHCPRELEASE                    0
     DHCPDECLINE                    0
     BOOTPREQUEST                   0
 Server -> Client:
     DHCPOFFER                      0
     DHCPACK                        0
     DHCPNAK                        0
```

```
BOOTPREPLY                      0
```

reset dhcp relay statistics

Syntax

reset dhcp relay statistics [**server-group** *group-id*]

View

User view

Default level

1: Monitor level

Parameters

server-group *group-id*: Specifies a server group ID (in the range of 0 to 19) about which to remove statistics from the relay agent.

Description

Use the **reset dhcp relay statistics** command to remove statistics from the relay agent.

If no **server-group** is specified, all statistics will be removed from the relay agent.

Related commands: **display dhcp relay statistics**.

Examples

Remove all statistics from the DHCP relay agent.

```
<Sysname> reset dhcp relay statistics
```

DHCP client configuration commands

NOTE:

- The DHCP client configuration is supported only on VLAN interfaces.
- When multiple VLAN interfaces having the same MAC address use DHCP for IP address acquisition via a relay agent, the DHCP server cannot be the Windows 2000 Server or Windows 2003 Server.

display dhcp client

Syntax

display dhcp client [**verbose**] [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

verbose: Specifies verbose DHCP client information to be displayed.

interface *interface-type interface-number*: Specifies an interface of which to display DHCP client information.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display dhcp client** command to display DHCP client information. If no **interface** *interface-type interface-number* is specified, DHCP client information of all interfaces will be displayed.

Examples

Display DHCP client information of all interfaces.

```
<Sysname> display dhcp client
Vlan-interface1 DHCP client information:
 Current machine state: BOUND
 Allocated IP: 40.1.1.20 255.255.255.0
 Allocated lease: 259200 seconds, T1: 129600 seconds, T2: 226800 seconds
 DHCP server: 40.1.1.2
```

Display verbose DHCP client information.

```
<Sysname> display dhcp client verbose
Vlan-interface1 DHCP client information:
 Current machine state: BOUND
 Allocated IP: 40.1.1.20 255.255.255.0
 Allocated lease: 259200 seconds, T1: 129600 seconds, T2: 226800 seconds
 Lease from 2005.08.13 15:37:59   to   2005.08.16 15:37:59
 DHCP server: 40.1.1.2
 Transaction ID: 0x1c09322d
 Default router: 40.1.1.2
 Classless static route:
   Destination: 1.1.0.1, Mask: 255.0.0.0, NextHop: 192.168.40.16
   Destination: 10.198.122.63, Mask: 255.255.255.255, NextHop: 192.168.40.16
 DNS server: 44.1.1.11
 DNS server: 44.1.1.12
 Domain name: ddd.com
 Boot server: 200.200.200.200  1.1.1.1
 Client ID: 3030-3066-2e65-3234-
            392e-3830-3438-2d56-
            6c61-6e2d-696e-7465-
            7266-6163-6531
T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.
```

Table 15 Output description

Field	Description
Vlan-interface1 DHCP client information	Information of the interface acting as the DHCP client
Current machine state	Current state of the DHCP client, which can be: • HALT: Indicates that the client stops applying for an IP address. • INIT: Indicates the initialization state. • SELECTING: Indicates that the client has sent out a DHCP-DISCOVER message in search of a DHCP server and is waiting for the response from DHCP servers. • REQUESTING: Indicates that the client has sent out a DHCP-REQUEST message requesting for an IP address and is waiting for the response from DHCP servers. • BOUND: Indicates that the client has received the DHCP-ACK message from a DHCP server and obtained an IP address successfully. • RENEWING: Indicates that the T1 timer expires. • REBOUNDING: Indicates that the T2 timer expires.
Allocated IP	The IP address allocated by the DHCP server
Allocated lease	The allocated lease time
T1	The 1/2 lease time (in seconds) of the DHCP client IP address
T2	The 7/8 lease time (in seconds) of the DHCP client IP address
Lease from….to….	The start and end time of the lease.
DHCP Server	DHCP server IP address that assigned the IP address

Field	Description
Transaction ID	Transaction ID, a random number chosen by the client to identify an IP address allocation.
Default router	The gateway address assigned to the client
Classless static route	Classless static routes assigned to the client
Static route	Classful static routes assigned to the client
DNS server	The DNS server address assigned to the client
Domain name	The domain name suffix assigned to the client
Boot server	PXE server addresses (up to 16 addresses) specified for the DHCP client, which are obtained through Option 43.
Client ID	Client ID
T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.	How long the T1 (1/2 lease time) timer will timeout.

ip address dhcp-alloc

Syntax

ip address dhcp-alloc [**client-identifier mac** *interface-type interface-number*]

undo ip address dhcp-alloc

View

Interface view

Default level

2: System level

Parameters

client-identifier mac *interface-type interface-number*: Specifies the MAC address of an interface using which as the client ID to obtain an IP address.

Description

Use the **ip address dhcp-alloc** command to configure an interface to use DHCP for IP address acquisition.

Use the **undo ip address dhcp-alloc** command to cancel an interface from using DHCP.

By default, an interface does not use DHCP for IP address acquisition.

If no parameter is specified, the client uses a character string comprised of the current interface name and MAC address as its ID for address acquisition.

The DHCP client sends a DHCP-RELEASE message for releasing the IP address obtained via DHCP, if the interface of the client is down, the message cannot be sent.

Examples

Configure VLAN-interface 1 to use DHCP for IP address acquisition.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip address dhcp-alloc
```

DHCP snooping configuration commands

NOTE:

The DHCP snooping enabled device does not work if it is between the DHCP relay agent and DHCP server, and it can work when it is between the DHCP client and relay agent or between the DHCP client and server.

dhcp-snooping

Syntax

dhcp-snooping

undo dhcp-snooping

View

System view

Default level

2: System level

Parameters

None

Description

Use the **dhcp-snooping** command to enable DHCP snooping.

Use the **undo dhcp-snooping** command to disable DHCP snooping.

With DHCP snooping disabled, all ports can forward responses from any DHCP servers and does not record binding information about MAC addresses of DHCP clients and the obtained IP addresses.

By default, DHCP snooping is disabled.

Related commands: **display dhcp-snooping**.

Examples

Enable DHCP snooping.

```
<Sysname> system-view
[Sysname] dhcp-snooping
```

dhcp-snooping binding database filename

Syntax

dhcp-snooping binding database filename *filename*

undo dhcp-snooping binding database filename

View

System view

Default level

2: System level

Parameters

filename: File name. For how to define the file name, see the *Fundamentals Configuration Guide*.

Description

Use the **dhcp-snooping binding database filename** command to specify the name of the file for storing DHCP snooping entries.

Use the **undo dhcp-snooping binding database filename** to restore the default.

By default, no file name is specified.

If no file with the specified name is found, the device will automatically create the file upon storing a DHCP snooping binding.

DHCP snooping entries are stored immediately after this command is used, and then updated at the interval set by the **dhcp-snooping binding database update interval** command.

Related commands: **dhcp-snooping binding database update interval**.

Examples

Specify the name of the file for storing DHCP snooping entries as **database.dhcp**.

```
<Sysname> system-view
[Sysname] dhcp-snooping binding database filename database.dhcp
```

dhcp-snooping binding database update interval

Syntax

dhcp-snooping binding database update interval *minutes*

undo dhcp-snooping binding database update interval

View

System view

Default level

2: System level

Parameters

minutes: Refresh interval in minutes, in the range of 1 to 14400.

Description

Use the **dhcp-snooping binding database update interval** command to set the interval at which the DHCP snooping entry file is refreshed.

Use the **undo dhcp-snooping binding database update interval** command to restore the default.

By default, the DHCP snooping entry file is not refreshed periodically.

With this command configured, DHCP snooping will check bindings periodically. If a binding is added or removed during an interval, DHCP snooping will add or remove this binding to or from the file at the end of this interval; if no change occurs within the interval, DHCP snooping will not refresh the file.

This command takes effect only when the DHCP snooping entry file is specified.

Configure the refresh interval shorter than the lease duration of IP addresses in the DHCP address pool.

Related commands: **dhcp-snooping binding database filename**.

Examples

Configure the DHCP snooping entry file to be refreshed every 10 minutes.

```
<Sysname> system-view
[Sysname] dhcp-snoooping binding database update interval 10
```

dhcp-snooping binding database update now

Syntax

dhcp-snooping binding database update now

View

System view

Default level

2: System level

Parameters

None

Description

Use the **dhcp-snooping binding database update now** command to store DHCP snooping entries to the file.

DHCP snooping entries will be stored to the file each time this command is used.

This command takes effect only when the DHCP snooping entry file is specified.

Related commands: **dhcp-snooping binding database filename**.

Examples

Store DHCP snooping entries to the file.

```
<Sysname> system-view
[Sysname] dhcp-snooping binding database update now
```

dhcp-snooping check mac-address

Syntax

dhcp-snooping check mac-address

undo dhcp-snooping check mac-address

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

None

Description

Use the **dhcp-snooping check mac-address** command to enable MAC address check on a DHCP snooping device.

Use the **undo dhcp-snooping check mac-address** command to disable MAC address check of DHCP snooping.

By default, this function is disabled.

With this function enabled, the DHCP snooping device compares the chaddr field of a received DHCP request with the source MAC address field in the frame. If they are the same, the DHCP snooping device decides this request valid and forwards it to the DHCP server. If not, the DHCP request is discarded.

Examples

Enable MAC address check of DHCP snooping.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping check mac-address
```

dhcp-snooping check request-message

Syntax

dhcp-snooping check request-message

undo dhcp-snooping check request-message

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

None

Description

Use the **dhcp-snooping check request-message** command to enable DHCP-REQUEST message check of DHCP snooping.

Use the **undo dhcp-snooping check request-message** command to disable DHCP-REQUEST message check of the DHCP snooping.

By default, this function is disabled.

With this function enabled, upon receiving a DHCP-REQUEST message, a DHCP snooping device searches local DHCP snooping entries for the corresponding entry of the message. If an entry is found, the DHCP snooping device compares the entry with the message information. If they are consistent, the DHCP-REQUEST message is considered as valid lease renewal request and forwarded to the DHCP server. If they are not consistent, the messages is considered as forged lease renewal request and discarded. If no corresponding entry is found locally, the message is considered valid and forwarded to the DHCP server.

Examples

Enable DHCP-REQUEST message check of DHCP snooping.

```
<Sysname> system-view
```

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping check request-message
```

dhcp-snooping information circuit-id format-type

Syntax

dhcp-snooping information circuit-id format-type { **ascii** | **hex** }

undo dhcp-snooping information circuit-id format-type

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

ascii: Specifies the code type for the circuit ID sub-option as **ascii**.

hex: Specifies the code type for the circuit ID sub-option as **hex**.

Description

Use the **dhcp-snooping information circuit-id format-type** command to configure the code type for the non-user-defined circuit ID sub-option.

Use the **undo dhcp-snooping information circuit-id format-type** command to restore the default.

By default, the code type for the circuit ID sub-option depends on the padding format of Option 82. Each field has its own code type.

This command applies to configuring the non-user-defined circuit ID sub-option only. After you configure the padding content for the circuit ID sub-option using the **dhcp-snooping information circuit-id string** command, ASCII is adopted as the code type.

Related commands: **display dhcp-snooping information**.

Examples

Configure the padding format for the non-user-defined circuit ID sub-option as **ascii**.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information circuit-id format-type ascii
```

dhcp-snooping information circuit-id string

Syntax

dhcp-snooping information [**vlan** *vlan-id*] **circuit-id string** *circuit-id*

undo dhcp-snooping information [**vlan** *vlan-id*] **circuit-id string**

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

vlan *vlan-id*: Specifies a VLAN ID, in the range of 1 to 4094.

circuit-id: Padding content for the user-defined circuit ID sub-option, a case-sensitive string of 3 to 63 characters.

Description

Use the **dhcp-snooping information circuit-id string** command to configure the padding content for the user-defined circuit ID sub-option.

Use the **undo dhcp-snooping information circuit-id string** command to restore the default.

By default, the padding content for the circuit ID sub-option depends on the padding format of Option 82.

After you configure the padding content for the circuit ID sub-option using this command, ASCII is adopted as the code type.

If a VLAN is specified, the configured circuit ID sub-option only takes effect within the VLAN; if no VLAN is specified, the configured circuit ID sub-option takes effect in all VLANs. The former case has a higher priority. The circuit ID sub-option specified for a VLAN will be padded for packets within the VLAN.

Related commands: **dhcp-snooping information format** and **display dhcp-snooping information**.

Examples

Configure the global padding content for the user-defined circuit ID sub-option as **company001**.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information circuit-id string company001
```

dhcp-snooping information enable

Syntax

dhcp-snooping information enable

undo dhcp-snooping information enable

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

None

Description

Use the **dhcp-snooping information enable** command to configure DHCP snooping to support Option 82.

Use the **undo dhcp-snooping information enable** command to disable this function.

By default, DHCP snooping does not support Option 82.

Related commands: **display dhcp-snooping information**.

Examples

Configure DHCP snooping to support Option 82.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information enable
```

dhcp-snooping information format

Syntax

dhcp-snooping information format { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] }

undo dhcp-snooping information format [**verbose node-identifier**]

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

normal: Specifies the normal padding format.

verbose: Specifies the verbose padding format.

node-identifier { **mac** | **sysname** | **user-defined** *node-identifier* }: Specifies access node identifier. By default, the node MAC address is used as the node identifier.

- **mac** indicates using MAC address as the node identifier.
- **sysname** indicates using the device name of a node as the node identifier.
- **user-defined** *node-identifier* indicates using a specified character string as the node identifier, in which *node-identifier* is a string of 1 to 50 characters.

Description

Use the **dhcp-snooping information format** command to specify the padding format for Option 82.

Use the **undo dhcp-snooping information format** command to restore the default.

By default, the padding format for Option 82 is **normal**.

When you use the **undo dhcp-snooping information format** command, if the **verbose node-identifier** argument is not specified, the padding format will be restored to **normal**; if the **verbose node-identifier** argument is specified, the padding format will be restored to **verbose** with MAC address as the node identifier.

Related commands: **display dhcp-snooping information**.

Examples

Specify the padding format as **verbose** for Option 82.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information enable
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information strategy replace
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information format verbose
```

dhcp-snooping information remote-id format-type

Syntax

dhcp-snooping information remote-id format-type { **ascii** | **hex** }

undo dhcp-snooping information remote-id format-type

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

ascii: Specifies the code type for the remote ID sub-option as **ascii**.

hex: Specifies the code type for the remote ID sub-option as **hex**.

Description

Use the **dhcp-snooping information remote-id format-type** command to configure the code type for the non-user-defined remote ID sub-option.

Use the **undo dhcp-snooping information remote-id format-type** command to restore the default.

By default, the code type for the remote ID sub-option is HEX.

This command applies to configuring a non-user-defined remote ID sub-option only. After you configure the padding content for the remote ID sub-option using the **dhcp-snooping information remote-id string** command, ASCII is adopted as the code type.

Related commands: **display dhcp-snooping information**.

Examples

Configure the code type for the non-user-defined remote ID sub-option as **ascii**.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information remote-id format-type ascii
```

dhcp-snooping information remote-id string

Syntax

dhcp-snooping information [**vlan** *vlan-id*] **remote-id string** { *remote-id* | **sysname** }

undo dhcp-snooping information [**vlan** *vlan-id*] **remote-id string**

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

vlan *vlan-id*: Specifies a VLAN ID, in the range of 1 to 4094.

remote-id: Padding content for the user-defined circuit ID sub-option, a case-sensitive string of 1 to 63 characters.

sysname: Specifies the device name as the padding content for the remote ID sub-option.

Description

Use the **dhcp-snooping information remote-id string** command to configure the padding content for the user-defined remote ID sub-option.

Use the **undo dhcp-snooping information remote-id string** command to restore the default.

By default, the padding content for the remote ID sub-option depends on the padding format of Option 82.

After you configure the padding content for the remote ID sub-option using this command, ASCII is adopted as the code type.

If a VLAN is specified, the configured remote ID sub-option only takes effect within the VLAN; if no VLAN is specified, the configured remote ID sub-option takes effect in all VLANs. The former case has a higher priority. The remote ID sub-option configured for a VLAN will be padded for the packets within the VLAN.

NOTE:

If you want to specify the character string **sysname** (a case-insensitive character string) as the padding content for the remote ID sub-option, you need to use quotation marks to make it take effect. For example, if you want to specify **Sysname** as the padding content for the remote ID sub-option, you need to enter the **dhcp relay information remote-id string** "Sysname" command.

Related commands: **dhcp-snooping information format** and **display dhcp-snooping information**.

Examples

Configure the padding content for the remote ID sub-option as **device001**.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information remote-id string device001
```

dhcp-snooping information strategy

Syntax

dhcp-snooping information strategy { **drop** | **keep** | **replace** }

undo dhcp-snooping information strategy

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

drop: Drops the requesting message containing Option 82.

keep: Forwards the requesting message containing Option 82 without changing Option 82.

replace: Forwards the requesting message containing Option 82 after replacing the original Option 82 with the one padded in specified format.

Description

Use the **dhcp-snooping information strategy** command to configure the handling strategy for Option 82 in requesting messages.

Use the **undo dhcp-snooping information strategy** command to restore the default.

By default, the handling strategy for Option 82 in requesting messages is **replace**.

Related commands: **display dhcp-snooping information**.

Examples

Configure the handling strategy for Option 82 in requesting messages as **keep**.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information enable
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information strategy keep
```

dhcp-snooping trust

Syntax

dhcp-snooping trust [**no-user-binding**]

undo dhcp-snooping trust

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

no-user-binding: Specifies the port not to record the clients' IP-to-MAC bindings in DHCP requests it receives. The command without this keyword records the IP-to-MAC bindings of clients.

Description

Use the **dhcp-snooping trust** command to configure a port as a trusted port.

Use the **undo dhcp-snooping trust** command to restore the default state of a port.

All ports are untrusted by default.

After enabling DHCP snooping, you need to specify the ports connected to the valid DHCP servers as trusted to ensure that DHCP clients can obtain valid IP addresses.

Related commands: **display dhcp-snooping trust**.

Examples

Specify GigabitEthernet 1/0/1 as a trusted port and enable it to record the IP-to-MAC bindings of clients.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping trust
```

display dhcp-snooping

Syntax

display dhcp-snooping [**ip** *ip-address*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

ip *ip-address*: Displays the DHCP snooping entries corresponding to the specified IP address.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display dhcp-snooping** command to display DHCP snooping entries.

NOTE:

Only the DHCP snooping entries containing IP-to-MAC bindings that are present both in the DHCP-ACK and DHCP-REQUEST messages are displayed by using the **display dhcp-snooping** command.

Related commands: **dhcp-snooping** and **reset dhcp-snooping**.

Examples

Display all DHCP snooping entries.

```
<Sysname> display dhcp-snooping
 DHCP Snooping is enabled.
 The client binding table for all untrusted ports.
 Type : D--Dynamic , S--Static
 Type IP Address       MAC Address      Lease      VLAN  Interface
 ==== ===============  ===============  ========== ==== =================
 D    10.1.1.1         00e0-fc00-0006   286          1    GigabitEthernet1/0/1
---   1 dhcp-snooping item(s) found   ---
```

Table 16 Output description

Field	Description
Type	Binding type, which can be: • D: Dynamic IP-to-MAC binding. • S: Static IP-to-MAC binding. Static IP-to-MAC bindings are not supported.
IP Address	IP address assigned to the DHCP client
MAC Address	MAC address of the DHCP client

Field	Description
Lease	Lease period left (in seconds)
VLAN	Outer VLAN tag when DHCP snooping and QinQ are both enabled or the DHCP snooping device receives a packet with two VLAN tags; or VLAN where the port connecting the DHCP client resides
Interface	Port to which the DHCP client is connected

display dhcp-snooping binding database

Syntax

display dhcp-snooping binding database [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display dhcp-snooping binding database** command to display the DHCP snooping entry file information.

Examples

Display the DHCP snooping entry file information.

```
<Sysname> display dhcp-snooping binding database
File name              :   flash:/database.dhcp
Update interval    :   10 minutes
Latest read time     :   Jul 15 2008 16:38:22
Latest write time      :   Jul 15 2008 16:38:24
Status             :   Last write succeeded.
```

Table 17 Output description

Field	Description
File name	File name
Update interval	Interval at which the DHCP snooping entry file is refreshed
Latest read time	The last time when the file is read
Latest write time	The last time when the file is written

Field	Description
Status	Indicates whether the file was written successfully last time

NOTE:

When the device reboots, the latest file write time and write status is cleared.

display dhcp-snooping information

Syntax

display dhcp-snooping information { **all** | **interface** *interface-type interface-number* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

all: Displays the Option 82 configuration information of all Layer 2 Ethernet interfaces.

interface *interface-type interface-number*: Displays the Option 82 configuration information of a specified interface.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display dhcp-snooping information** command to display Option 82 configuration information on the DHCP snooping device.

Examples

Display the Option 82 configuration information of all interfaces.

```
<Sysname> display dhcp-snooping information all
Interface: GigabitEthernet 1/0/1
    Status: Enable
    Strategy: Replace
    Format: Verbose
    Circuit ID format-type: HEX
    Remote ID format-type: ASCII
    Node identifier: aabbcc
    User defined:
        Circuit ID: company001
Interface: GigabitEthernet 1/0/2
```

```
Status: Disable
Strategy: Keep
Format: Normal
Circuit ID format-type: HEX
Remote ID format-type: ASCII
User defined:
    Circuit ID: company001
    Remote ID: device001
    VLAN 10:
        Circuit ID: vlan10@company001
    VLAN 20:
        Remote ID: device001
```

display dhcp-snooping packet statistics

Syntax

display dhcp-snooping packet statistics [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

slot *slot-number*: Displays the DHCP packet statistics of the specified device. If the device is in an IRF, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF, the *slot-number* argument represents the device ID.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters

Description

Use the **display dhcp-snooping packet statistics** command to display DHCP packet statistics on the DHCP snooping device.

Related commands: **reset dhcp-snooping packet statistics**.

Examples

Display DHCP packet statistics on the DHCP snooping device.

```
<Sysname> display dhcp-snooping packet statistics
 DHCP packets received                  : 100
 DHCP packets sent                      : 200
 Packets dropped due to rate limitation : 20
 Dropped invalid packets                : 0
```

display dhcp-snooping trust

Syntax

display dhcp-snooping trust [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display dhcp-snooping trust** command to display information about trusted ports.

Related commands: **dhcp-snooping trust**.

Examples

Display information about trusted ports.

```
<Sysname> display dhcp-snooping trust
 DHCP Snooping is enabled.
 DHCP Snooping trust becomes active.
 Interface                                   Trusted
 ========================                  ============
 GigabitEthernet1/0/1                        Trusted
```

The above output shows that DHCP snooping is enabled, DHCP snooping trust is active, and port GigabitEthernet1/0/1 is trusted.

reset dhcp-snooping

Syntax

reset dhcp-snooping { **all** | **ip** *ip-address* }

View

User view

Default level

1: Monitor level

Parameters

all: Clears all DHCP snooping entries.

ip *ip-address*: Clears the DHCP snooping entries of the specified IP address.

Description

Use the **reset dhcp-snooping** command to clear DHCP snooping entries.

Related commands: **display dhcp-snooping**.

Examples

Clear all DHCP snooping entries.

```
<Sysname> reset dhcp-snooping all
```

reset dhcp-snooping packet statistics

Syntax

reset dhcp-snooping packet statistics [**slot** *slot-number*]

View

User view

Default level

2: System level

Parameters

slot *slot-number*: Clears the DHCP packet statistics of the specified device. If the device is in an IRF, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF, the *slot-number* argument represents the device ID.

Description

Use the **reset dhcp-snooping packet statistics** command to clear DHCP packet statistics on the DHCP snooping device.

Related commands: **display dhcp-snooping packet statistics**.

Examples

Clear DHCP packet statistics on the DHCP snooping device.

```
<Sysname> reset dhcp-snooping packet statistics
```

BOOTP client configuration commands

NOTE:

- BOOTP client configuration can only be used on VLAN interfaces.
- If several VLAN interfaces sharing the same MAC address obtain IP addresses through a BOOTP relay agent, the BOOTP server cannot be a Windows 2000 Server or Windows 2003 Server.

display bootp client

Syntax

display bootp client [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface *interface-type interface-number*: Displays the BOOTP client information of the interface.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display bootp client** command to display related information about a BOOTP client.

Note the following:

- If **interface** *interface-type interface-number* is not specified, the command will display information about BOOTP clients on all interfaces.
- If **interface** *interface-type interface-number* is specified, the command will display information about the BOOTP client on the specified interface.

Examples

Display related information of the BOOTP client on VLAN-interface 1.

```
<Sysname> display bootp client interface vlan-interface 1
Vlan-interface1 BOOTP client information:
Allocated IP: 169.254.0.2 255.255.0.0
Transaction ID = 0x3d8a7431
Mac Address  00e0-fc0a-c3ef
```

Table 18 Output description

Field	Description
Vlan-interface1 BOOTP client information	Information of the interface serving as a BOOTP client
Allocated IP	BOOTP client's IP address allocated by the BOOTP server
Transaction ID	Value of the **XID** field in a BOOTP message, which is a random number chosen when the BOOTP client sends a BOOTP request to the BOOTP server. It is used to match a response message from the BOOTP server. If the values of the **XID** field are different in the BOOTP response and request, the BOOTP client will drop the BOOTP response.
Mac Address	MAC address of a BOOTP client

ip address bootp-alloc

Syntax

ip address bootp-alloc

undo ip address bootp-alloc

View

Interface view

Default level

2: System level

Parameters

None

Description

Use the **ip address bootp-alloc** command to enable an interface to obtain an IP address through BOOTP.

Use the **undo ip address bootp-alloc** command to disable the interface from obtaining an IP address through BOOTP.

By default, an interface does not obtain an IP address through BOOTP.

Related commands: **display bootp client**.

Examples

Configure VLAN-interface 1 to obtain IP address through BOOTP protocol.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip address bootp-alloc
```

IPv4 DNS configuration commands

display dns domain

Syntax

display dns domain [**dynamic**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

dynamic: Displays the domain name suffixes dynamically obtained through DHCP or other protocols.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display dns domain** command to display the domain name suffixes.

Related commands: **dns domain**.

Examples

Display domain name suffixes.

```
<Sysname> display dns domain
 Type:
  D:Dynamic    S:Static

No.     Type    Domain-name
1       S       com
```

Table 19 Output description

Field	Description
No	Sequence number
Type	Type of domain name suffix: S represents a statically configured domain name suffix, and D represents a domain name suffix obtained dynamically through DHCP.
Domain-name	Domain name suffix

display dns host

Syntax

display dns host [**ip** | **ipv6** | **naptr** | **srv**] [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

ip: Displays the dynamic cache information of type A queries. A type A query resolves a domain name to the mapped IPv4 address.

ipv6: Displays the dynamic cache information of type AAAA queries. A type AAAA query resolves a domain name to the mapped IPv6 address.

naptr: Displays the dynamic cache information of NAPTR queries. A NAPTR query offers the replacement rule of a character string to convert the character string to a domain name.

srv: Displays the dynamic cache information of SRV queries. An SRV query offers the domain name of a certain service site.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display dns host** command to display the dynamic DNS cache information.

Without any keyword specified, the dynamic DNS cache information of all query types will be displayed.

Related commands: **reset dns host**.

Examples

Display the dynamic DNS cache information of all query types.

```
<Sysname> display dns host
No.  Host                      TTL  Type  Reply Data
1    sample.com                3132 IP    192.168.10.1
2    sample.net                2925 IPv6  FE80::4904:4448
3    sip.sample.com            3122 NAPTR 100 10 u sip+E2U !^.*$!sip:info.se!i
4    website.tcp.sample.com    3029 SRV   10 10 8080 iis.sample.com
```

Table 20 Output description

Field	Description
No	Sequence number

Field	Description
Host	Domain name for query
TTL	Time that a mapping can be stored in the cache (in seconds)
Type	Query type, including IP, IPv6, NAPTR, and SRV
Reply Data	Reply data concerning the query type: • For an IP query, the reply data is an IPv4 address. • For an IPv6 query, the reply data is an IPv6 address. • For a NAPTR query, the reply data comprises order, preference, flags, services, regular expression, and replacement. • For an SRV query, the reply data comprises the priority, weight, port, and target domain name.

display dns server

Syntax

display dns server [**dynamic**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

dynamic: Displays the DNS server information dynamically obtained through DHCP or other protocols

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display dns server** command to display the IPv4 DNS server information.

Related commands: **dns server**.

Examples

Display the IPv4 DNS server information.

```
<Sysname> display dns server
 Type:
  D:Dynamic    S:Static

DNS Server  Type  IP Address
    1       S     169.254.65.125
```

Table 21 Output description

Field	Description
DNS Server	Sequence number of the DNS server, configured automatically by the device, starting from 1.
Type	Type of domain name server: **S** represents a statically configured DNS server, and **D** represents a DNS server obtained dynamically through DHCP.
IP Address	IPv4 address of the DNS server

display ip host

Syntax

display ip host [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display ip host** command to display the host names and corresponding IPv4 addresses in the static domain name resolution table.

Examples

Display the host names and corresponding IPv4 addresses in the static domain name resolution table.

```
<Sysname> display ip host
Host         Age      Flags        Address
My           0        static       1.1.1.1
Aa           0        static       2.2.2.4
```

Table 22 Output description

Field	Description
Host	Host name
Age	Time to live. 0 means that the static mapping will never age out. You can only manually remove the static mappings between host names and IPv4 addresses.

Field	Description
Flags	Indicates the mapping type. Static represents static IPv4 domain name resolution.
Address	Host IPv4 address

dns domain

Syntax

dns domain *domain-name*

undo dns domain [*domain-name*]

View

System view

Default level

2: System level

Parameters

domain-name: Domain name suffix, consisting of character strings separated by a dot (for example, aabbcc.com). Each separated string contains no more than 63 characters. A domain name suffix may include case-insensitive letters, digits, hyphens (-), underscores (_), and dots (.), with a total length of 238 characters.

Description

Use the **dns domain** command to configure a domain name suffix. The system can automatically add the suffix to part of the domain name you entered for resolution.

Use the **undo dns domain** command to delete a domain name suffix (with a domain name suffix specified) or all domain name suffixes (with no domain name suffix specified).

No domain name suffix is configured by default. Only the provided domain name is resolved.

NOTE:

- The domain name suffix configured with the **dns domain** command is applicable to both IPv4 DNS and IPv6 DNS.
- You can configure a maximum of 10 domain name suffixes.

Related commands: **display dns domain**.

Examples

Configure com as a DNS suffix.

```
<Sysname> system-view
[Sysname] dns domain com
```

dns proxy enable

Syntax

dns proxy enable

undo dns proxy enable

View

System view

Default level

2: System level

Parameters

None

Description

Use the **dns proxy enable** command to enable DNS proxy.

Use the **undo dns proxy enable** command to disable DNS proxy.

By default, DNS proxy is disabled.

Examples

Enable DNS proxy.

```
<Sysname> system-view
[Sysname] dns proxy enable
```

dns resolve

Syntax

dns resolve

undo dns resolve

View

System view

Default level

2: System level

Parameters

None

Description

Use the **dns resolve** command to enable dynamic domain name resolution.

Use the **undo dns resolve** command to disable dynamic domain name resolution.

Dynamic domain name resolution is disabled by default.

This command is applicable to both IPv4 DNS and IPv6 DNS.

Examples

Enable dynamic domain name resolution.

```
<Sysname> system-view
[Sysname] dns resolve
```

dns server

Syntax

In system view:

dns server *ip-address*

undo dns server [*ip-address*]

In interface view:

dns server *ip-address*

undo dns server *ip-address*

View

System view, interface view

Default level

2: System level

Parameters

ip-address: IPv4 address of the DNS server.

Description

Use the **dns server** command to specify a DNS server.

Use the **undo dns server** to remove DNS server(s).

No DNS server is specified by default.

NOTE:

- In system view, you can configure up to six DNS servers, including those with IPv6 addresses. The total number of DNS servers configured in interface view must be within six.
- Running the **undo dns server** command in system view will delete all DNS servers configured in system view and interface view. Running the **undo dns server** *ip-address* command in system view or interface view will delete the specific DNS server in system view or interface view.
- The DNS server configured in system view has a higher priority than the DNS server configured in interface view. A name query request is first sent to each DNS server configured in system view; if no rely is obtained, the request is sent to each DNS server configured in interface view in turn.

Related commands: **display dns server**.

Examples

Specify the DNS server 172.16.1.1 in system view.

```
<Sysname> system-view
[Sysname] dns server 172.16.1.1
```

dns source-interface

Syntax

dns source-interface *interface-type interface-number*

undo dns source-interface

View

System view

Default level

2: System level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Description

Use **dns source-interface** to specify the source interface for DNS packets.

Use **undo dns source-interface** to restore the default.

By default, no source interface for DNS packets is specified. The device uses the primary IP address of the output interface of the matching route as the source IP address of a DNS request.

The device uses the primary IP address of the specified source interface as the source IP address of a DNS request, which however is still forwarded through the output interface of the matching route.

Examples

Specify VLAN-interface 2 as the source interface of DNS requests.

```
<Sysname> system-view
[Sysname] dns source-interface vlan-interface 2
```

dns spoofing

Syntax

dns spoofing *ip-address*

undo dns spoofing

View

System view

Default level

2: System level

Parameters

ip-address: IP address used to spoof name query requests.

Description

Use the **dns spoofing** command to enable DNS spoofing.

Use the **undo dns spoofing** command to disable DNS spoofing.

By default, DNS spoofing is disabled.

With DNS proxy enabled but no DNS server specified or no DNS server reachable, a switch cannot forward a DNS request, or answer the request. In this case, you can enable DNS spoofing on the switch to spoof a reply with the configured IP address. Once a DNS server is reachable, the switch will send DNS requests to the server and return replies to the requesting DNS clients.

If you repeatedly execute the **dns spoofing** command with different IP addresses specified, the latest configuration will overwrite the previous one.

Examples

Enable DNS spoofing and specify the IP address as 1.1.1.1

```
<Sysname> system-view
[Sysname] dns spoofing 1.1.1.1
```

ip host

Syntax

ip host *hostname ip-address*

undo ip host *hostname* [*ip-address*]

View

System view

Default level

2: System level

Parameters

hostname: Host name, consisting of 1 to 255 characters, including case-insensitive letters, numbers, hyphens (-), underscores (_), or dots (.). The host name must include at least one letter.

ip-address: IPv4 address of the specified host in dotted decimal notation.

Description

Use the **ip host** command to create a host name to IPv4 address mapping in the static resolution table.

Use the **undo ip host** command to remove a mapping.

No mappings are created by default.

Each host name can correspond to only one IPv4 address. The IPv4 address you last assign to the host name will overwrite the previous one if there is any.

Related commands: **display ip host**.

Examples

Map the IP address 10.110.0.1 to the host name aaa.

```
<Sysname> system-view
[Sysname] ip host aaa 10.110.0.1
```

reset dns host

Syntax

reset dns host [**ip** | **ipv6** | **naptr** | **srv**]

View

User view

Default level

2: System level

Parameters

ip: Clears the dynamic cache information of type A queries. A type A query resolves a domain name to the mapped IPv4 address.

ipv6: Clears the dynamic cache information of type AAAA queries. A type AAAA query resolves a domain name to the mapped IPv6 address.

naptr: Clears the dynamic cache information of NAPTR queries. A NAPTR query offers the replacement rule of a character string to convert the character string to a domain name.

srv: Clears the dynamic cache information of SRV queries. An SRV query offers the domain name of a certain service site.

Description

Use the **reset dns host** command to clear information of the dynamic DNS cache.

Without any keyword specified, the dynamic DNS cache information of all query types will be cleared.

Related commands: **display dns host**.

Examples

Clear the dynamic DNS cache information of all query types.

```
<Sysname> reset dns host
```

IPv6 DNS configuration commands

display dns ipv6 server

Syntax

display dns ipv6 server [**dynamic**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

dynamic: Displays IPv6 DNS server information acquired dynamically through DHCP or other protocols.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display dns ipv6 server** command to display IPv6 DNS server information.

Examples

Display IPv6 DNS server information.

```
<Sysname> display dns ipv6 server
 Type:
  D:Dynamic    S:Static

DNS Server  Type  IPv6 Address                              (Interface Name)
    1       S     1::1
    2       S     FE80::1                                  Vlan999
```

Table 23 Output description

Field	Description
DNS Server	Sequence number of the DNS server, which is assigned automatically by the system, starting from 1.
Type	Type of the DNS server: "S" represents a statically configured DNS server, and "D" represents a DNS server obtained dynamically through DHCP or other protocols.
IPv6 Address	IPv6 address of the DNS server
Interface Name	Interface name, which is available only for a DNS server with an IPv6 link-local address configured.

display ipv6 host

Syntax

display ipv6 host [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display ipv6 host** command to display the mappings between host names and IPv6 addresses in the static domain name resolution table.

Related commands: **ipv6 host**.

Examples

Display the mappings between host names and IPv6 addresses in the static domain name resolution table.

```
<Sysname> display ipv6 host
Host                   Age         Flags           IPv6Address
aaa                    0           static           2002::1
bbb                    0           static           2002::2
```

Table 24 Output description

Field	Description
Host	Host name
Age	Time for the entry to live. "0" is displayed in the case of static configuration.
Flags	Type of the mapping. Static indicates a static mapping.
IPv6Address	IPv6 address of a host

dns server ipv6

Syntax

dns server ipv6 *ipv6-address* [*interface-type interface-number*]

undo dns server ipv6 *ipv6-address* [*interface-type interface-number*]

View

System view

Default level

2: System level

Parameters

ipv6-address: IPv6 address of a DNS server.

interface-type interface-number: Specifies an interface. When the IPv6 address of the DNS server is a link-local address, the two arguments must be specified.

Description

Use the **dns server ipv6** command to specify a DNS server.

Use the **undo dns server ipv6** command to remove the specified DNS server.

By default, no DNS server is configured.

You can configure a maximum of six DNS servers, including those with IPv4 addresses.

Examples

Specify a DNS server at 2002::1.

```
<Sysname> system-view
[Sysname] dns server ipv6 2002::1
```

ipv6 host

Syntax

ipv6 host *hostname ipv6-address*

undo ipv6 host *hostname* [*ipv6-address*]

View

System view

Default level

2: System level

Parameters

hostname: Host name, a string of up to 255 characters. The character string can contain letters, numbers, underscores (_), hyphens (-), or dots (.) and must contain at least one letter.

ipv6-address: IPv6 address.

Description

Use the **ipv6 host** command to configure a mapping between host name and IPv6 address.

Use the **undo ipv6 host** command to remove a mapping between host name and IPv6 address.

No mappings are created by default.

Each host name can correspond to only one IPv6 address. The IPv6 address you last assign to the host name will overwrite the previous one if there is any.

Related commands: **display ipv6 host**.

Examples

Configure the mapping between a host name and an IPv6 address.

```
<Sysname> system-view
[Sysname] ipv6 host aaa 2001::1
```

IP performance optimization configuration commands

display fib

Syntax

display fib [**acl** *acl-number* | **ip-prefix** *ip-prefix-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

acl *acl-number*: Displays FIB entries matching a specified ACL numbered from 2000 to 2999. If the specified ACL does not exist, all FIB entries are displayed.

ip-prefix *ip-prefix-name*: Displays FIB entries matching a specified IP prefix list, a string of 1 to 19 characters. If the specified IP prefix list does not exist, all FIB entries are displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display fib** command to display FIB entries. If no parameters are specified, all FIB entries will be displayed.

Examples

Display all FIB entries.

```
<Sysname> display fib
Destination count: 4    FIB entry count: 4

Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay

Destination/Mask  Nexthop     Flag    OutInterface  InnerLabel Token
10.2.0.0/16       10.2.1.1    U       Vlan1         Null       Invalid
10.2.1.1/32       127.0.0.1   UH      InLoop0       Null       Invalid
```

```
127.0.0.0/8       127.0.0.1   U       InLoop0       Null       Invalid
127.0.0.1/32      127.0.0.1   UH      InLoop0       Null       Invalid
```

Display FIB information passing ACL 2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.2.0.0 0.0.255.255
[Sysname-acl-basic-2000] display fib acl 2000
Destination count: 2    FIB entry count: 2

 Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay

Destination/Mask  Nexthop     Flag    OutInterface  InnerLabel Token
10.2.0.0/16       10.2.1.1    U       Vlan1         Null       Invalid
10.2.1.1/32       127.0.0.1   UH      InLoop0       Null       Invalid
```

Display all entries that contain the string **127** and start from the first one.

```
<Sysname> display fib | begin 127
Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay

Destination/Mask  Nexthop     Flag    OutInterface  InnerLabel Token
10.2.1.1/32       127.0.0.1   UH      InLoop0       Null       Invalid
127.0.0.0/8       127.0.0.1   U       InLoop0       Null       Invalid
127.0.0.1/32      127.0.0.1   UH      InLoop0       Null       Invalid
```

Table 25 Output description

Field	Description
Destination count	Total number of destination addresses
FIB entry count	Total number of FIB entries
Destination/Mask	Destination address/length of mask
Nexthop	Next hop address
Flag	Flags of routes: • **U**—Usable route • **G**—Gateway route • **H**—Host route • **B**—Blackhole route • **D**—Dynamic route • **S**—Static route • **R**—Relay route
OutInterface	Outbound interface
InnerLabel	Inner label
Token	Link-state packet (LSP) index number

display fib *ip-address*

Syntax

display fib *ip-address* [*mask* | *mask-length*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

ip-address: Destination IP address, in dotted decimal notation.

mask: IP address mask.

mask-length: Length of IP address mask.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display fib** *ip-address* command to display FIB entries that match the specified destination IP address.

If no mask or mask length is specified, the FIB entry that matches the destination IP address and has the longest mask will be displayed; if the mask is specified, the FIB entry that exactly matches the specified destination IP address will be displayed.

Examples

Display the FIB entries that match the destination IP address of 10.2.1.1.

```
<Sysname> display fib 10.2.1.1
Destination count: 1    FIB entry count: 1

Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay

Destination/Mask  Nexthop     Flag     OutInterface  InnerLabel Token
10.2.1.1/32       127.0.0.1   UH       InLoop0       Null       Invalid
```

For description about the output, see Table 25.

display icmp statistics

Syntax

display icmp statistics [**slot** *slot-number*] [**|** { **begin** | **include** | **exclude** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

slot *slot-number*: Displays the ICMP statistics on the specified device. If the device is in an IRF, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF, the *slot-number* argument represents the device ID.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display icmp statistics** command to display ICMP statistics.

Related commands: **display ip interface** (IP addressing configuration commands in the *Layer 3—IP Services Command Reference*); **reset ip statistics** (IP performance optimization configuration commands in the *Layer 3—IP Services Command Reference*).

Examples

Display ICMP statistics.

```
<Sysname> display icmp statistics
  Input: bad formats   0                  bad checksum            0
         echo          5                  destination unreachable 0
         source quench 0                  redirects               0
         echo reply    10                 parameter problem       0
         timestamp     0                  information request     0
         mask requests 0                  mask replies            0
         time exceeded 0
  Output:echo          10                 destination unreachable 0
         source quench 0                  redirects               0
         echo reply    5                  parameter problem       0
         timestamp     0                  information reply       0
         mask requests 0                  mask replies            0
         time exceeded 0
```

Table 26 Output description

Field	Description
bad formats	Number of input wrong format packets
bad checksum	Number of input wrong checksum packets
echo	Number of input/output echo packets
destination unreachable	Number of input/output destination unreachable packets

Field	Description
source quench	Number of input/output source quench packets
redirects	Number of input/output redirection packets
echo reply	Number of input/output replies
parameter problem	Number of input/output parameter problem packets
timestamp	Number of input/output time stamp packets
information request	Number of input information request packets
mask requests	Number of input/output mask requests
mask replies	Number of input/output mask replies
information reply	Number of output information reply packets
time exceeded	Number of input/output expiration packets

display ip socket

Syntax

display ip socket [**socktype** *sock-type*] [*task-id socket-id*] [**slot** *slot-number*] [**|** { **begin** | **include** | **exclude** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

socktype *sock-type*: Displays the socket information of this type. The sock type is in the range 1 to 3, corresponding to TCP, UDP and raw IP respectively.

task-id: Displays the socket information of this task. Task ID is in the range 1 to 180.

socket-id: Displays the information of the socket. Socket ID is in the range 0 to 3072.

slot *slot-number*: Displays the socket information of the specified device. If the device is in an IRF, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF, the *slot-number* argument represents the device ID.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display ip socket** command to display socket information.

Examples

Display the TCP socket information.

```
<Sysname> display ip socket
SOCK_STREAM:
Task = VTYD(38), 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_SETKEEPALIVE,
socket state = SS_PRIV SS_ASYNC

Task = HTTP(36), socketid = 1, Proto = 6,
LA = 0.0.0.0:80, FA = 0.0.0.0:0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT,
socket state = SS_PRIV SS_NBIO

Task = ROUT(69), socketid = 10, Proto = 6,
LA = 0.0.0.0:179, FA = 192.168.1.45:0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEADDR SO_REUSEPORT
socket state = SS_PRIV SS_ASYNC

Task = VTYD(38), socketid = 4, Proto = 6,
LA = 192.168.1.40:23, FA = 192.168.1.52:1917,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 237, rb_cc = 0,
socket option = SO_KEEPALIVE SO_OOBINLINE SO_REUSEPORT SO_SETKEEPALIVE,
socket state = SS_ISCONNECTED SS_PRIV SS_ASYNC

Task = VTYD(38), socketid = 3, Proto = 6,
LA = 192.168.1.40:23, FA = 192.168.1.84:1503,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_KEEPALIVE SO_OOBINLINE SO_REUSEPORT SO_SETKEEPALIVE,
socket state = SS_ISCONNECTED SS_PRIV SS_ASYNC

Task = ROUT(69), socketid = 11, Proto = 6,
LA = 192.168.1.40:1025, FA = 192.168.1.45:179,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_REUSEADDR SO_LINGER,
socket state = SS_ISCONNECTED SS_PRIV SS_ASYNC

SOCK_DGRAM:
Task = NTPT(37), socketid = 1, Proto = 17,
LA = 0.0.0.0:123, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 41600, sb_cc = 0, rb_cc = 0,
socket option = SO_UDPCHECKSUM,
socket state = SS_PRIV

Task = AGNT(51), socketid = 1, Proto = 17,
```

```
LA = 0.0.0.0:161, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 41600, sb_cc = 0, rb_cc = 0,
socket option = SO_UDPCHECKSUM,
socket state = SS_PRIV SS_NBIO SS_ASYNC

Task = RDSO(56), socketid = 1, Proto = 17,
LA = 0.0.0.0:1024, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 41600, sb_cc = 0, rb_cc = 0,
socket option = SO_UDPCHECKSUM,
socket state = SS_PRIV

Task = TRAP(52), socketid = 1, Proto = 17,
LA = 0.0.0.0:1025, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 0, sb_cc = 0, rb_cc = 0,
socket option = SO_UDPCHECKSUM,
socket state = SS_PRIV

Task = RDSO(56), socketid = 2, Proto = 17,
LA = 0.0.0.0:1812, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 41600, sb_cc = 0, rb_cc = 0,
socket option = SO_UDPCHECKSUM,
socket state = SS_PRIV

SOCK_RAW:
Task = ROUT(69), socketid = 8, Proto = 89,
LA = 0.0.0.0, FA = 0.0.0.0,
sndbuf = 262144, rcvbuf = 262144, sb_cc = 0, rb_cc = 0,
socket option = SO_UDPCHECKSUM,
socket state = SS_PRIV SS_ASYNC

Task = ROUT(69), socketid = 3, Proto = 2,
LA = 0.0.0.0, FA = 0.0.0.0,
sndbuf = 32767, rcvbuf = 256000, sb_cc = 0, rb_cc = 0,
socket option = SO_UDPCHECKSUM,
socket state = SS_PRIV SS_NBIO SS_ASYNC

Task = ROUT(69), socketid = 2, Proto = 103,
LA = 0.0.0.0, FA = 0.0.0.0,
sndbuf = 65536, rcvbuf = 256000, sb_cc = 0, rb_cc = 0,
socket option = SO_UDPCHECKSUM,
socket state = SS_PRIV SS_NBIO SS_ASYNC

Task = ROUT(69), socketid = 1, Proto = 65,
LA = 0.0.0.0, FA = 0.0.0.0,
sndbuf = 32767, rcvbuf = 256000, sb_cc = 0, rb_cc = 0,
socket option = 0,
socket state = SS_PRIV SS_NBIO SS_ASYNC
```

```
Task = RSVP(73), 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
```

Table 27 Output description

Field	Description
SOCK_STREAM	TCP socket
SOCK_DGRAM	UDP socket
SOCK_RAW	Raw IP socket
Task	Task number
socketid	Socket ID
Proto	Protocol number of the socket, indicating the protocol type that IP carries
LA	Local address and local port number
FA	Remote address and remote port number
sndbuf	Sending buffer size of the socket, in bytes
rcvbuf	Receiving buffer size of the socket, in bytes
sb_cc	Current data size in the sending buffer (It is available only for TCP that can buffer data)
rb_cc	Data size currently in the receiving buffer
socket option	Socket option
socket state	Socket state

display ip statistics

Syntax

display ip statistics [**slot** *slot-number*] [**|** { **begin** | **include** | **exclude** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

slot *slot-number*: Displays statistics of IP packets on the specified device. If the device is in an IRF, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF, the *slot-number* argument represents the device ID.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display ip statistics** command to display statistics of IP packets.

Related commands: **display ip interface** (IP addressing configuration commands in the *Layer 3—IP Services Command Reference*); **reset ip statistics** (IP performance optimization configuration commands in the *Layer 3—IP Services Command Reference*).

Examples

Display statistics of IP packets.

```
<Sysname> display ip statistics
  Input:    sum            7120             local            112
            bad protocol   0                bad format       0
            bad checksum   0                bad options      0
  Output:   forwarding     0                local            27
            dropped        0                no route         2
            compress fails 0
  Fragment:input           0                output           0
            dropped        0
            fragmented     0                couldn't fragment 0
  Reassembling:sum         0                timeouts         0
```

Table 28 Output description

Field		Description
Input:	sum	Total number of packets received
	local	Total number of packets with destination being local
	bad protocol	Total number of unknown protocol packets
	bad format	Total number of packets with incorrect format
	bad checksum	Total number of packets with incorrect checksum
	bad options	Total number of packets with incorrect option
Output:	forwarding	Total number of packets forwarded
	local	Total number of packets sent from the local
	dropped	Total number of packets discarded
	no route	Total number of packets for which no route is available
	compress fails	Total number of packets failed to be compressed
Fragment:	input	Total number of fragments received
	output	Total number of fragments sent
	dropped	Total number of fragments dropped
	fragmented	Total number of packets successfully fragmented
	couldn't fragment	Total number of packets that failed to be fragmented
Reassembling	sum	Total number of packets reassembled
	timeouts	Total number of reassembly timeout fragments

display tcp statistics

Syntax

display tcp statistics [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display tcp statistics** command to display statistics of TCP traffic.

Related commands: **display tcp status** and **reset tcp statistics**.

Examples

Display statistics of TCP traffic.

```
<Sysname> display tcp statistics
Received packets:
     Total: 8457
     packets in sequence: 3660 (5272 bytes)
     window probe packets: 0, window update packets: 0
     checksum error: 0, offset error: 0, short error: 0

     duplicate packets: 1 (8 bytes), partially duplicate packets: 0 (0 bytes)
     out-of-order packets: 17 (0 bytes)
     packets of data after window: 0 (0 bytes)
     packets received after close: 0

     ACK packets: 4625 (141989 bytes)
     duplicate ACK packets: 1702, too much ACK packets: 0

Sent packets:
     Total: 6726
     urgent packets: 0
     control packets: 21 (including 0 RST)
     window probe packets: 0, window update packets: 0

     data packets: 6484 (141984 bytes) data packets retransmitted: 0 (0 bytes)
```

```
    ACK-only packets: 221 (177 delayed)

Retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
Keepalive timeout: 1682, keepalive probe: 1682, Keepalive timeout, so connections
disconnected : 0
Initiated connections: 0, accepted connections: 22, established connections: 22
Closed connections: 49 (dropped: 0, initiated dropped: 0)
Packets dropped with MD5 authentication: 0
Packets permitted with MD5 authentication: 0
```

Table 29 Output description

Field		Description
Received packets	Total	Total number of packets received
	packets in sequence	Number of packets arriving in sequence
	window probe packets	Number of window probe packets received
	window update packets	Number of window update packets received
	checksum error	Number of checksum error packets received
	offset error	Number of offset error packets received
	short error	Number of received packets with length being too small
	duplicate packets	Number of completely duplicate packets received
	partially duplicate packets	Number of partially duplicate packets received
	out-of-order packets	Number of out-of-order packets received
	packets of data after window	Number of packets outside the receiving window
	packets received after close	Number of packets that arrived after connection is closed
	ACK packets	Number of ACK packets received
	duplicate ACK packets	Number of duplicate ACK packets received
	too much ACK packets	Number of ACK packets for data unsent
Sent packets	Total	Total number of packets sent
	urgent packets	Number of urgent packets sent
	control packets	Number of control packets sent
	window probe packets	Number of window probe packets sent; in the brackets are resent packets
	window update packets	Number of window update packets sent
	data packets	Number of data packets sent
	data packets retransmitted	Number of data packets retransmitted
	ACK-only packets	Number of ACK packets sent; in brackets are delayed ACK packets
Retransmitted timeout		Number of retransmission timer timeouts
connections dropped in retransmitted timeout		Number of connections broken due to retransmission timeouts
Keepalive timeout		Number of keepalive timer timeouts

Field	Description
keepalive probe	Number of keepalive probe packets sent
Keepalive timeout, so connections disconnected	Number of connections broken due to timeout of the keepalive timer
Initiated connections	Number of connections initiated
accepted connections	Number of connections accepted
established connections	Number of connections established
Closed connections	Number of connections closed; in brackets are connections closed accidentally (before receiving SYN from the peer) and connections closed initiatively (after receiving SYN from the peer)
Packets dropped with MD5 authentication	Number of packets dropped by MD5 authentication
Packets permitted with MD5 authentication	Number of packets permitted by MD5 authentication

display udp statistics

Syntax

display udp statistics [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display udp statistics** command to display statistics of UDP packets.

Related commands: **reset udp statistics**.

Examples

Display statistics of UDP packets.

```
<Sysname> display udp statistics
Received packets:
     Total: 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
```

Table 30 Output description

Field		Description
Received packets:	Total	Total number of UDP packets received
	checksum error	Total number of packets with incorrect checksum
	shorter than header	Number of packets with data shorter than head
	data length larger than packet	Number of packets with data longer than packet
	unicast(no socket on port)	Number of unicast packets with no socket on port
	broadcast/multicast(no socket on port)	Number of broadcast/multicast packets without socket on port
	not delivered, input socket full	Number of packets not delivered to an upper layer due to a full socket cache
	input packets missing pcb cache	Number of packets without matching protocol control block (PCB) cache
Sent packets:	Total	Total number of UDP packets sent

ip forward-broadcast (interface view)

Syntax

ip forward-broadcast [**acl** *acl-number*]

undo ip forward-broadcast

View

Interface view

Default level

2: System level

Parameters

acl *acl-number*: Access control list number, in the range 2000 to 3999. From 2000 to 2999 are numbers for basic ACLs, and from 3000 to 3999 are numbers for advanced ACLs. Only directed broadcasts permitted by the ACL can be forwarded.

Description

Use the **ip forward-broadcast** command to enable the interface to forward directed broadcasts to a directly-connected network.

Use the **undo ip forward-broadcast** command to disable the interface from forwarding directed broadcasts to a directly-connected network.

By default, an interface is disabled from forwarding directed broadcasts to a directly-connected network.

Examples

Enable VLAN-interface 2 to forward the directed broadcasts to a directly-connected network matching ACL 2001.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ip forward-broadcast acl 2001
```

ip forward-broadcast (system view)

Syntax

ip forward-broadcast

undo ip forward-broadcast

View

System view

Default level

2: System level

Parameters

None

Description

Use the **ip forward-broadcast** command to enable the switch to receive directed broadcasts.

Use the **undo ip forward-broadcast** command to disable the switch from receiving directed broadcasts.

By default, the switch is disabled from receiving directed broadcasts..

Examples

Enable the switch to receive directed broadcasts.

```
<Sysname> system-view
[Sysname] ip forward-broadcast
```

ip ttl-expires enable

Syntax

ip ttl-expires enable

undo ip ttl-expires

View

System view

Default level

2: System level

Parameters

None

Description

Use the **ip ttl-expires enable** command to enable sending of ICMP timeout packets.

Use the **undo ip ttl-expires** command to disable sending of ICMP timeout packets.

Sending ICMP timeout packets is disabled by default.

If the feature is disabled, the switch will not send TTL timeout ICMP packets, but still send "reassembly timeout" ICMP packets.

Examples

Enable sending of ICMP timeout packets.

```
<Sysname> system-view
[Sysname] ip ttl-expires enable
```

ip unreachables enable

Syntax

ip unreachables enable

undo ip unreachables

View

System view

Default level

2: System level

Parameters

None

Description

Use the **ip unreachables enable** command to enable sending of ICMP destination unreachable packets.

Use the **undo ip unreachables** command to disable sending of ICMP destination unreachable packets.

Sending ICMP destination unreachable packets is disabled by default.

Examples

Enable sending of ICMP destination unreachable packets.

```
<Sysname> system-view
[Sysname] ip unreachables enable
```

reset ip statistics

Syntax

reset ip statistics [**slot** *slot-number*]

View

User view

Default level

2: System level

Parameters

slot *slot-number*: Clears IP packet statistics on the specified device. If the device is in an IRF, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF, the *slot-number* argument represents the device ID.

Description

Use the **reset ip statistics** command to clear statistics of IP packets.

Related commands: **display ip interface** (IP addressing configuration commands in the *Layer 3—IP Services Command Reference*); **display ip statistics** (IP performance optimization configuration commands in the *Layer 3—IP Services Command Reference*).

Examples

Clear statistics of IP packets.

```
<Sysname> reset ip statistics
```

reset tcp statistics

Syntax

reset tcp statistics

View

User view

Default level

2: System level

Parameters

None

Description

Use the **reset tcp statistics** command to clear statistics of TCP traffic.

Related commands: **display tcp statistics**.

Examples

Display statistics of TCP traffic.

```
<Sysname> reset tcp statistics
```

reset udp statistics

Syntax

reset udp statistics

View

User view

Default level

2: System level

Parameters

None

Description

Use the **reset udp statistics** command to clear statistics of UDP traffic.

Examples

Display statistics of UDP traffic.

```
<Sysname> reset udp statistics
```

tcp timer fin-timeout

Syntax

tcp timer fin-timeout *time-value*

undo tcp timer fin-timeout

View

System view

Default level

2: System level

Parameters

time-value: Length of the TCP finwait timer in seconds, in the range 76 to 3,600.

Description

Use the **tcp timer fin-timeout** command to configure the length of the TCP finwait timer.

Use the **undo tcp timer fin-timeout** command to restore the default.

By default, the length of the TCP finwait timer is 675 seconds.

Note that the actual length of the finwait timer is determined by the following formula:

Actual length of the finwait timer = (Configured length of the finwait timer – 75) + configured length of the synwait timer

Related commands: **tcp timer syn-timeout** and **tcp window**.

Examples

Set the length of the TCP finwait timer to 800 seconds.

```
<Sysname> system-view
[Sysname] tcp timer fin-timeout 800
```

tcp timer syn-timeout

Syntax

tcp timer syn-timeout *time-value*

undo tcp timer syn-timeout

View

System view

Default level

2: System level

Parameters

time-value: TCP finwait timer in seconds, in the range 2 to 600.

Description

Use the **tcp timer syn-timeout** command to configure the length of the TCP synwait timer.

Use the **undo tcp timer syn-timeout** command to restore the default.

By default, the value of the TCP synwait timer is 75 seconds.

Related commands: **tcp timer fin-timeout** and **tcp window**.

Examples

Set the length of the TCP synwait timer to 80 seconds.

```
<Sysname> system-view
[Sysname] tcp timer syn-timeout 80
```

tcp window

Syntax

tcp window *window-size*

undo tcp window

View

System view

Default level

2: System level

Parameters

window-size: Size of the send/receive buffer in KB, in the range 1 to 32.

Description

Use the **tcp window** command to configure the size of the TCP send/receive buffer.

Use the **undo tcp window** command to restore the default.

The size of the TCP send/receive buffer is 8 KB by default.

Related commands: **tcp timer fin-timeout** and **tcp timer syn-timeout**.

Examples

Configure the size of the TCP send/receive buffer as 3 KB.

```
<Sysname> system-view
[Sysname] tcp window 3
```

UDP Helper configuration commands

display udp-helper server

Syntax

display udp-helper server [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

interface *interface-type interface-number*: Displays information of forwarded UDP packets on the specified interface.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display udp-helper server** command to display the information of forwarded UDP packets on the specified interface or all interfaces.

If *interface-type interface-number* is not specified, this command displays the information of forwarded UDP packets on all interfaces.

Examples

Display the information of forwarded UDP packets on the interface VLAN-interface 1.

```
<Sysname> display udp-helper server interface vlan-interface 1
Interface name      Server address      Packets sent
Vlan-interface1     192.1.1.2           0
```

The information above shows that the IP address of the destination server corresponding to the interface VLAN-interface 1 is 192.1.1.2, and that no packets are forwarded to the destination server.

reset udp-helper packet

Syntax

reset udp-helper packet

View

User view

Default level

2: System level

Parameters

None

Description

Use the **reset udp-helper packet** command to clear the statistics of UDP packets forwarded.

Related commands: **display udp-helper server**.

Examples

Clear the statistics of the forwarded UDP packets.

```
<Sysname> reset udp-helper packet
```

udp-helper enable

Syntax

udp-helper enable

undo udp-helper enable

View

System view

Default level

2: System level

Parameters

None

Description

Use the **udp-helper enable** command to enable UDP Helper. The switch enabled with UDP Helper functions as a relay agent that converts UDP broadcast packets into unicast packets and forwards them to a specified destination server.

Use the **undo udp-helper enable** command to disable UDP Helper.

By default, UDP Helper is disabled.

Examples

Enable UDP Helper

```
<Sysname> system-view
[Sysname] udp-helper enable
```

udp-helper port

Syntax

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** }

View

System view

Default level

2: System level

Parameters

port-number: UDP port number with which packets need to be forwarded, in the range of 1 to 65535 (except 67 and 68).

dns: Forwards DNS data packets. The corresponding UDP port number is 53.

netbios-ds: Forwards NetBIOS data packets. The corresponding UDP port number is 138.

netbios-ns: Forwards NetBIOS name service data packets. The corresponding UDP port number is 137.

tacacs: Forwards terminal access controller access control system (TACACS) data packet. The corresponding UDP port number is 49.

tftp: Forwards TFTP data packets. The corresponding UDP port number is 69.

time: Forwards time service data packets. The corresponding UDP port number is 37.

Description

Use the **udp-helper port** command to enable the forwarding of packets with the specified UDP port number.

Use the **undo udp-helper port** command to remove the configured UDP port numbers.

By default, no UDP port number is specified.

The specified UDP port numbers will all be removed if UDP Helper is disabled.

Examples

Forward broadcast packets with the UDP destination port number 100.

```
<Sysname> system-view
[Sysname] udp-helper port 100
```

udp-helper server

Syntax

udp-helper server *ip-address*

undo udp-helper server [*ip-address*]

View

Interface view

Default level

2: System level

Parameters

ip-address: IP address of the destination server, in dotted decimal notation.

Description

Use the **udp-helper server** command to specify the destination server which UDP packets need to be forwarded to.

Use the **undo udp-helper server** command to remove the destination server.

No destination server is configured by default.

You can configure up to 20 destination servers on an interface.

Without the *ip-address* argument, the **undo udp-helper server** command removes all the destination servers on an interface.

Related commands: **display udp-helper server**.

Examples

Specify the IP address of the destination server as 192.1.1.2 on the interface VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] udp-helper server 192.1.1.2
```

IPv6 basics configuration commands

display ipv6 fib

Syntax

display ipv6 fib [**slot** *slot-number*] [*ipv6-address*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

slot-number: Displays the IPv6 forwarding information base (FIB) entries of a specified device in an IRF. If no IRF is formed, the IPv6 FIB entries of the current device are displayed only. The *slot-number* argument indicates the member ID of the device.

ipv6-address: Displays the IPv6 FIB entries containing the specified destination IPv6 address.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display ipv6 fib** command to display IPv6 FIB entries. If no argument is specified, all IPv6 FIB entries will be displayed.

The device looks up a matching IPv6 FIB entry for forwarding an IPv6 packet.

Examples

Display all IPv6 FIB entries.

```
<Sysname> display ipv6 fib
FIB Table:
 Total number of Routes : 1

 Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static

Destination:    ::1                                  PrefixLength : 128
NextHop    :    ::1                                  Flag         : HU
Label      :    NULL                                 Tunnel ID    : 0
TimeStamp  :    Date- 7/14/2007, Time- 15:17:15
Interface  :    InLoopBack0
```

Table 31 Output description

Field	Description
Total number of Routes	Total number of routes in the FIB
Destination	Destination address
PrefixLength	Prefix length of the destination address
NextHop	Next hop
Flag	Route flag: • **U**—Usable route • **G**—Gateway route • **H**—Host route • **B**—Black hole route • **D**—Dynamic route • **S**—Static route
Label	Label
Tunnel ID	ID of a tunnel
TimeStamp	Generation time of a FIB entry
Interface	Outgoing interface

display ipv6 fibcache

Syntax

display ipv6 fibcache *slot-number*[**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

slot-number: Displays the number of routes in the FIB cache of the specified IRF member device. The *slot-number* is the ID of the IRF member device. You can use the **display irf** command to view the IDs of IRF member devices. If no IRF is formed, the *slot-number* is the number of the current device.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display ipv6 fibcache** command to display the number of routes in the IPv6 FIB cache.

Examples

Display the number of routes in the FIB cache.

```
<Sysname> display ipv6 fibcache 1
FIB Cache:
 Total number of Routes : 0
```

display ipv6 interface

Syntax

display ipv6 interface [*interface-type* [*interface-number*]] [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface-type: Interface type.

interface-number: Interface number.

verbose: Displays the detailed IPv6 information of an interface.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display ipv6 interface** command to display the IPv6 information of an interface.

If *interface-type interface-number* is not specified, the IPv6 information of all interfaces is displayed; if only *interface-type* is specified, the IPv6 information of the interfaces of the specified type is displayed; if *interface-type interface-number* is specified, the IPv6 information of the specified interface is displayed. If the **verbose** keyword is also specified, the detailed IPv6 information of the interface is displayed.

Examples

Display the IPv6 information of VLAN-interface 2.

```
<Sysname> display ipv6 interface vlan-interface 2 verbose
Vlan-interface2 current state :UP
Line protocol current state :UP
IPv6 is enabled, link-local address is FE80::1234:56FF:FE65:4322
  Global unicast address(es):
    2001::1, subnet is 2001::/64
10::1234:56FF:FE65:4322, subnet is 10::/64 [AUTOCFG]
      [valid lifetime 4641s/preferred lifetime 4637s]
  Joined group address(es):
```

```
    FF02::1:FF00:1
    FF02::1:FF65:4322
    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
  Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
  InReceives:                    0
  InTooShorts:                   0
  InTruncatedPkts:               0
  InHopLimitExceeds:             0
  InBadHeaders:                  0
  InBadOptions:                  0
  ReasmReqds:                    0
  ReasmOKs:                      0
  InFragDrops:                   0
  InFragTimeouts:                0
  OutFragFails:                  0
  InUnknownProtos:               0
  InDelivers:                    0
  OutRequests:                   0
  OutForwDatagrams:              0
  InNoRoutes:                    0
  InTooBigErrors:                0
  OutFragOKs:                    0
  OutFragCreates:                0
  InMcastPkts:                   0
  InMcastNotMembers:             0
  OutMcastPkts:                  0
  InAddrErrors:                  0
  InDiscards:                    0
  OutDiscards:                   0
```

Table 32 Output description

Field	Description
Vlan-interface2 current state	Physical state of the interface: • Administratively DOWN: Indicates that the VLAN interface is administratively down. The interface is shut down by using the **shutdown** command. • DOWN: Indicates that the VLAN interface is administratively up but its physical state is down. No ports in the VLAN are up due to a connection or link failure. • UP: Indicates that the administrative and physical states of the VLAN interface are both up.

Field	Description
Line protocol current state	Link layer protocol state of the interface: • DOWN: Indicates that the link layer protocol state of the VLAN interface is down. • UP: Indicates that the link layer protocol state of the VLAN interface is up.
IPv6 is enabled	IPv6 packet forwarding state of the interface (after an IPv6 address is configured for an interface, IPv6 is automatically enabled on it; IPv6 packet forwarding is enabled in the example)
link-local address	Link-local address configured for the interface
Global unicast address(es)	Global unicast address(es) configured for the interface
valid lifetime	Valid lifetime of the global unicast address obtained through stateless autoconfiguration
preferred lifetime	Preferred lifetime of the global unicast address obtained through stateless autoconfiguration
Joined group address(es)	Address(es) of multicast group(s) that the interface has joined
MTU	Maximum transmission unit of the interface
ND DAD is enabled, number of DAD attempts	Whether Duplicate Address Detection (DAD) is enabled. In this example, DAD is enabled. • If DAD is enabled, the number of attempts to send a Neighbor Solicitation (NS) message for DAD (configured by using the **ipv6 nd dad attempts** command) is also displayed. • If DAD is disabled, **ND DAD is disabled** is displayed. (You can disable DAD by setting the number of attempts to send an NS message for DAD to 0.)
ND reachable time	Time that a neighboring node is considered reachable after reachability has been confirmed
ND retransmit interval	Interval for retransmitting an NS message
Hosts use stateless autoconfig for addresses	Hosts use stateless autoconfiguration mode to acquire IPv6 addresses
InReceives	All IPv6 packets received by the interface, including all types of error packets.
InTooShorts	Received IPv6 packets that are too short, with a length less than 40 bytes, for example.
InTruncatedPkts	Received IPv6 packets with a length less than that specified in the packets
InHopLimitExceeds	Received IPv6 packets with a hop count exceeding the limit
InBadHeaders	Received IPv6 packets with bad basic headers
InBadOptions	Received IPv6 packets with bad extension headers
ReasmReqds	Received IPv6 fragments
ReasmOKs	Number of packets after reassembly rather than the number of fragments
InFragDrops	IPv6 fragments discarded due to certain error
InFragTimeouts	IPv6 fragments discarded because the interval for which they had stayed in the system buffer exceeded the specified period

Field	Description
OutFragFails	Packets failed in fragmentation on the outbound interface
InUnknownProtos	Received IPv6 packets with unknown or unsupported protocol type
InDelivers	Received IPv6 packets that were delivered to application layer protocols (such as ICMPv6, TCP, and UDP)
OutRequests	Local IPv6 packets sent by IPv6 application protocols
OutForwDatagrams	Packets forwarded by the outbound interface.
InNoRoutes	IPv6 packets that were discarded because no matched route can be found
InTooBigErrors	IPv6 packets that were discarded because they exceeded the PMTU
OutFragOKs	Packets that were fragmented on the outbound interface
OutFragCreates	Number of packet fragments after fragmentation on the outbound interface
InMcastPkts	IPv6 multicast packets received on the interface
InMcastNotMembers	Incoming IPv6 multicast packets that were discarded because the interface did not belong to the corresponding multicast groups
OutMcastPkts	IPv6 multicast packets sent by the interface
InAddrErrors	IPv6 packets that were discarded due to invalid destination addresses
InDiscards	Received IPv6 packets that were discarded due to resource problems rather than packet content errors
OutDiscards	Sent packets that were discarded due to resource problems rather than packet content errors

Display the brief IPv6 information of all interfaces.

```
<Sysname> display ipv6 interface
*down: administratively down
(s): spoofing
Interface                      Physical     Protocol     IPv6 Address
Vlan-interface1                down         down         Unassigned
Vlan-interface2                up           up           2001::1
Vlan-interface100              up           down         Unassigned
```

Table 33 Output description

Field	Description
*down: administratively down	The interface is down. The interface is shut down by using the **shutdown** command.
(s): spoofing	Spoofing attribute of the interface. The link protocol state of the interface is up, but the link does not exist, or the link is established on demand, instead of being permanent.
Interface	Name of the interface

Field	Description
Physical	Physical state of the interface: • *down: Indicates that the VLAN interface is administratively down. The interface is shut down by using the **shutdown** command. • down: Indicates that the VLAN interface is administratively up but its physical state is down. No port in the VLAN is up due to a connection or link failure. • up: Indicates that the administrative and physical states of the VLAN interface are both up.
Protocol	Link layer protocol state of the interface: • down: Indicates that the network layer protocol state of the VLAN interface is down. • up: Indicates that the network layer protocol state of the VLAN interface is up.
IPv6 Address	IPv6 address of the interface. Only the first of configured IPv6 addresses is displayed. If no address is configured for the interface, **Unassigned** will be displayed.

display ipv6 nd snooping

Syntax

display ipv6 nd snooping [*ipv6-address* | **vlan** *vlan-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

ipv6-address: Specifies an IPv6 address.

vlan *vlan-id*: Displays ND snooping entries in the specified VLAN whose ID ranges from 1 to 4094.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display ipv6 nd snooping** command to display ND snooping entries.

Note that if no parameter is specified, this command displays all ND snooping entries.

Examples

Display the ND snooping entries of VLAN 1.

```
<Sysname> display ipv6 nd snooping vlan 1
```

```
IPv6 Address                   MAC Address     VID  Interface      Aging Status
4001::1                        0015-e944-a947  1    GE1/0/1         25    Bound
 ---- Total entries on VLAN 1: 1 ----
```

Table 34 Output description

Field	Description
IPv6 Address	IPv6 address of an ND snooping entry
MAC Address	MAC address of an ND snooping entry
VID	VLAN ID
Interface	Receiving port of an ND snooping entry
Aging	Aging time of an ND snooping entry, in minutes.
Status	ND snooping entry status, which can be Bound or Probe.
Total entries on VLAN 1	Total number of ND snooping entries of VLAN 1.

display ipv6 neighbors

Syntax

display ipv6 neighbors { { *ipv6-address* | **all** | **dynamic** | **static** } [**slot** *slot-number*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

ipv6-address: IPv6 address whose neighbor information is to be displayed.

all: Displays information of all neighbors, including neighbors acquired dynamically and configured statically.

dynamic: Displays information of all neighbors acquired dynamically.

static: Displays information of all neighbors configured statically.

slot *slot-number*: Displays information of the neighbors of a specified device in an IRF. If no IRF is formed, the neighbors of the current device are displayed only. The *slot-number* argument indicates the member ID of the device.

interface *interface-type interface-number*: Displays information of the neighbors of a specified interface.

vlan *vlan-id*: Displays information of the neighbors of a specified VLAN whose ID ranges from 1 to 4094.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display ipv6 neighbors** command to display neighbor information.

You can use the **reset ipv6 neighbors** command to clear specific IPv6 neighbor information.

Related commands: **ipv6 neighbor**, **reset ipv6 neighbors**.

Examples

Display all neighbor information.

```
<Sysname> display ipv6 neighbors all
                Type: S-Static    D-Dynamic
IPv6 Address            Link-layer      VID   Interface State T   Age
FE80::200:5EFF:FE32:B800  0000-5e32-b800  N/A GE1/0/1    REACH S    -
```

Table 35 Output description

Field	Description
IPv6 Address	IPv6 address of a neighbor
Link-layer	Link layer address (MAC address) of a neighbor
VID	VLAN to which the interface connected with a neighbor belongs
Interface	Interface connected with a neighbor
State	State of a neighbor, including: • INCMP: The address is being resolved. The link layer address of the neighbor is unknown. • REACH: The neighbor is reachable. • STALE: The reachability of the neighbor is unknown. The switch will not verify the reachability any longer unless data is sent to the neighbor. • DELAY: The reachability of the neighbor is unknown. The switch sends an NS message after a delay. • PROBE: The reachability of the neighbor is unknown. The switch sends an NS message to verify the reachability of the neighbor.
T	Type of neighbor information, including static configuration (represented by **S**) and dynamic acquisition (represented by **D**).
Age	For a static entry, a hyphen (-) is displayed. For a dynamic entry, the reachable time (in seconds) elapsed is displayed, and if it is never reachable, a number sign (#) is displayed (for a neighbor acquired dynamically).

display ipv6 neighbors count

Syntax

display ipv6 neighbors { { **all** | **dynamic** | **static** } [**slot** *slot-number*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } **count** [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

all: Displays the total number of all neighbor entries, including neighbor entries acquired dynamically and configured statically.

dynamic: Displays the total number of all neighbor entries acquired dynamically.

static: Displays the total number of neighbor entries configured statically.

slot *slot-number*: Displays the total number of neighbor entries of a specified device in an IRF. If no IRF is formed, the total number of neighbor entries of the current device is displayed only. The *slot-number* argument indicates the member ID of the device.

interface *interface-type interface-number*: Displays the total number of neighbor entries of a specified interface.

vlan *vlan-id*: Displays the total number of neighbor entries of a specified VLAN whose ID ranges from 1 to 4094.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display ipv6 neighbors count** command to display the total number of neighbor entries satisfying the specified condition.

Examples

Display the total number of neighbor entries acquired dynamically.

```
<Sysname> display ipv6 neighbors dynamic count
Total dynamic entry(ies):  2
```

display ipv6 pathmtu

Syntax

display ipv6 pathmtu { *ipv6-address* | **all** | **dynamic** | **static** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

ipv6-address: Destination IPv6 address for which the PMTU information is to be displayed.

all: Displays all PMTU information.

dynamic: Displays all dynamic PMTU information.

static: Displays all static PMTU information.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display ipv6 pathmtu** command to display the IPv6 PMTU information.

Examples

Display all PMTU information.

```
<Sysname> display ipv6 pathmtu all
IPv6 Destination Address ZoneID   PathMTU     Age      Type
 fe80::12                0        1300        40       Dynamic
 2222::3                 0        1280        --       Static
```

Table 36 Output description

Field	Description
IPv6 Destination Address	Destination IPv6 address
ZoneID	ID of address zone, currently invalid
PathMTU	Path MTU (PMTU) value on the network path to an IPv6 address
Age	Time for a PMTU to live. For a static PMTU, two consecutive hyphens (–) are displayed.
Type	Indicates that the PMTU is dynamically negotiated or statically configured.

display ipv6 socket

Syntax

display ipv6 socket [**socktype** *socket-type*] [*task-id socket-id*] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

socktype *socket-type*: Displays the socket information of this type. The socket type is in the range of 1 to 3. Value 1 represents a TCP socket, value 2 a UDP socket, and value 3 a raw socket.

task-id: Displays the socket information of the task. The task ID is in the range 1 to 150.

socket-id: Displays the information of the socket. The socket ID is in the range 0 to 3072.

slot *slot-number*: Displays the socket information of a specified device in an IRF. If no IRF is formed, the socket information of the current device is displayed only. The *slot-number* argument indicates the member ID of the device.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display ipv6 socket** command to display socket information.

With no parameter specified, this command displays the information about all the sockets; with only the socket type specified, the command displays the information about sockets of the specified type; with the socket type, task ID and socket ID specified, the command displays the information about the specified socket.

Examples

Display the information of all sockets.

```
<Sysname> display ipv6 socket
SOCK_STREAM:
Task = VTYD(14), socketid = 4, Proto = 6,
LA = ::->22, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT,
socket state = SS_PRIV SS_ASYNC

Task = VTYD(14), socketid = 3, Proto = 6,
LA = ::->23, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT,
socket state = SS_PRIV SS_ASYNC

SOCK_DGRAM:
Task = AGNT(51), socketid = 2, Proto = 17,
LA = ::->161, FA = ::->0,
sndbuf = 9216, rcvbuf = 42080, sb_cc = 0, rb_cc = 0,
socket option = SO_REUSEPORT,
socket state = SS_PRIV SS_NBIO SS_ASYNC

Task = TRAP(52), socketid = 2, Proto = 17,
LA = ::->1024, FA = ::->0,
sndbuf = 9216, rcvbuf = 42080, sb_cc = 0, rb_cc = 0,
socket option =,
socket state = SS_PRIV

SOCK_RAW:
```

```
Task = ROUT(86), socketid = 5, Proto = 89,
LA = ::, FA = ::,
sndbuf = 262144, rcvbuf = 262144, sb_cc = 0, rb_cc = 0,
socket option = SO_REUSEADDR,
socket state = SS_PRIV SS_ASYNC
```

Table 37 Output description

Field	Description
SOCK_STREAM	TCP socket
SOCK_DGRAM	UDP socket
SOCK_RAW	Raw IP socket
Task	Task name and ID of the created socket
socketid	ID assigned by the kernel to the created socket
Proto	Protocol type, for example, **6** indicates TCP and **17** indicates UDP.
LA	Local address and local port number
FA	Remote address and remote port number
sndbuf	Size of the send buffer
rcvbuf	Size of the receive buffer
sb_cc	Number of bytes sent by the send buffer
rb_cc	Number of bytes received by the receive buffer
socket option	Socket option set by the application, which can be: • SO_ACCEPTCONN: Detects connection request at the server end. • SO_REUSEADDR: Allows for reuse of a local address. • SO_REUSEPORT: Allows for reuse of a local port.
socket state	State of the socket

display ipv6 statistics

Syntax

display ipv6 statistics [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

slot *slot-number*: Displays statistics of IPv6 packets and ICMPv6 packets on a specified device in an IRF. If no IRF is formed, related information of the current device is displayed only. The *slot-number* argument indicates the member ID of the device.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display ipv6 statistics** command to display statistics of IPv6 packets and ICMPv6 packets.

You can use the **reset ipv6 statistics** command to clear all IPv6 and ICMPv6 packet statistics.

Examples

Display the statistics of IPv6 packets and ICMPv6 packets.

```
<Sysname> display ipv6 statistics
  IPv6 Protocol:

    Sent packets:
      Total:      0
        Local sent out:          0            forwarded:          0
        raw packets:         0            discarded:          0
        routing failed:          0            fragments:          0
        fragments failed:        0

    Received packets:
      Total:      0
        local host:          0            hopcount exceeded:  0
        format error:            0            option error:       0
        protocol error:          0            fragments:          0
        reassembled:         0            reassembly failed:  0
        reassembly timeout:      0

  ICMPv6 protocol:

    Sent packets:
      Total:      0
        unreached:           0              too big:            0
        hopcount exceeded:   0              reassembly timeout: 0
        parameter problem:   0
        echo request:        0              echo replied:       0
        neighbor solicit:    0              neighbor advert:    0
        router solicit:      0              router advert:      0
        redirected:      0
      Send failed:
        ratelimited:     0              other errors:     0

    Received packets:
      Total:      0
        checksum error:      0              too short:          0
        bad code:            0
        unreached:           0              too big:            0
        hopcount exceeded:   0              reassembly timeout: 0
```

```
    parameter problem:   0              unknown error type:    0
    echo request:        0              echo replied:          0
    neighbor solicit:    0              neighbor advert:       0
    router solicit:      0              router advert:         0
    redirected:      0              router renumbering:    0
    unknown info type:   0
  Deliver failed:
    bad length:      0              ratelimited:           0
```

Table 38 Output description

Field	Description
IPv6 Protocol:	Statistics of IPv6 packets
Sent packets: Total: 0 Local sent out: 0 forwarded: 0 raw packets: 0 discarded: 0 routing failed: 0 fragments: 0 fragments failed: 0	Statistics of sent IPv6 packets, including: • Total number of packets sent and forwarded locally • Number of packets sent locally • Number of forwarded packets • Number of packets sent via raw socket • Number of discarded packets • Number of packets failing to be routed • Number of sent fragment packets • Number of fragments failing to be sent
Received packets: Total: 0 local host: 0 hopcount exceeded: 0 format error: 0 option error: 0 protocol error:0 fragments: 0 reassembled: 0 reassembly failed: 0 reassembly timeout: 0	Statistics of received IPv6 packets, including • Total number of received packets • Number of packets received locally • Number of packets exceeding the hop limit • Number of packets in an incorrect format • Number of packets with incorrect options • Number of packets with incorrect protocol • Number of received fragment packets • Number of reassembled packets • Number of packets failing to be reassembled • Number of packets whose reassembly times out
ICMPv6 protocol:	Statistics of ICMPv6 packets

Field	Description
Sent packets: Total: 0 unreached: 0 too big: 0 hopcount exceeded: 0 reassembly timeout: 0 parameter problem: 0 echo request: 0 echo replied: 0 neighbor solicit: 0 neighbor advert: 0 router solicit: 0 router advert 0 redirected: 0 Send failed: ratelimited: 0 other errors: 0	Statistics of sent ICMPv6 packets, including • Total number of sent packets • Number of Destination Unreachable packets • Number of Packet Too Big packets • Number of Hop Limit Exceeded packets • Number of Fragment Reassembly Time Exceeded packets • Number of Parameter Problem packets • Number of Echo Request packets • Number of Echo Reply packets • Number of neighbor solicitation packets • Number of neighbor advertisement packets • Number of router solicitation packets • Number of router advertisement packets • Number of Redirect packets • Number of packets failing to be sent due to rate limitation • Number of packets with other errors
Received packets: Total: 0 checksum error: 0 too short: 0 bad code: 0 unreached: 0 too big: 0 hopcount exceeded: 0 reassembly timeout: 0 parameter problem: 0 unknown error type: 0 echo request: 0 echo replied: 0 neighbor solicit: 0 neighbor advert: 0 router solicit: 0 router advert 0 redirected: 0 router renumbering 0 unknown info type: 0 Deliver failed: bad length: 0 ratelimited: 0	Statistics of received ICMPv6 packets, including • Total number of received packets • Number of packets with checksum errors • Number of too small packets • Number of packets with error codes • Number of Destination Unreachable packets • Number of Packet Too Big packets • Number of Hop Limit Exceeded packets • Number of Fragment Reassembly Times Exceeded packets • Number of Parameter Problem packets • Number of packets with unknown errors • Number of Echo Request packets • Number of Echo Reply packets • Number of neighbor solicitation messages • Number of neighbor advertisement packets • Number of router solicitation packets • Number of router advertisement packets • Number of Redirect packets • Number of packets recounted by the router • Number of unknown type of packets • Number of packets with a incorrect size • Number of packets failing to be received due to rate limitation

display tcp ipv6 statistics

Syntax

display tcp ipv6 statistics [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display tcp ipv6 statistics** command to display IPv6 TCP connection statistics.

You can use the **reset tcp ipv6 statistics** command to clear statistics of all IPv6 TCP packets.

Examples

Display the statistics of IPv6 TCP connections.

```
<Sysname> display tcp ipv6 statistics
Received packets:
     Total: 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

Sent packets:
     Total: 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)
```

```
Retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
Keepalive timeout: 0, keepalive probe: 0, Keepalive timeout, so connections disconnected :
0
Initiated connections: 0, accepted connections: 0, established connections: 0
Closed connections: 0 (dropped: 0, initiated dropped: 0)
Packets dropped with MD5 authentication: 0
Packets permitted with MD5 authentication: 0
```

Table 39 Output description

Field	Description
Received packets: Total: 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	Statistics of received packets, including • Total number of received packets • Number of packets received in sequence • Number of window probe packets • Number of window size update packets • Number of packets with checksum errors • Number of packets with offset errors • Number of packets whose total length is less than specified by the packet header • Number of duplicate packets • Number of partially duplicate packets • Number of out-of-order packets • Number of packets exceeding the size of the receiving window • Number of packets received after the connection is closed • Number of ACK packets • Number of duplicate ACK packets • Number of excessive ACK packets
Sent packets: Total: 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)	Statistics of sent packets, including • Total number of packets • Number of packets containing an urgent indicator • Number of control packets • Number of window probe packets • Number of window update packets • Number of data packets • Number of retransmitted packets • Number of ACK packets
Retransmitted timeout	Number of packets whose retransmission times out
connections dropped in retransmitted timeout	Number of connections dropped because of retransmission timeout
Keepalive timeout	Number of keepalive timeouts

Field	Description
keepalive probe	Number of keepalive probes
Keepalive timeout, so connections disconnected	Number of connections dropped because of keepalive response 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 dropped connections (after SYN is received from the peer)
initiated dropped	Number of initiated but dropped connections (before SYN is received from the peer)
Packets dropped with MD5 authentication	Number of packets that fail the MD5 authentication and are dropped
Packets permitted with MD5 authentication	Number of packets that pass the MD5 authentication

display tcp ipv6 status

Syntax

display tcp ipv6 status [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display tcp ipv6 status** command to display the IPv6 TCP connection status, including the IPv6 TCP control block address, local and peer IPv6 addresses, and status of the IPv6 TCP connection.

Examples

Display the IPv6 TCP connection status.

```
*: TCP6 MD5 Connection
TCP6CB   Local Address            Foreign Address          State
1be2d8e0 ::->23                   ::->0                    Listening
1bde4530 ::->80                   ::->0                    Listening
```

Table 40 Output description

Field	Description
*: TCP6 MD5 Connection	The asterisk (*) indicates that the TCP6 connection is secured with MD5 authentication
TCP6CB	IPv6 TCP control block address (hexadecimal)
Local Address	Local IPv6 address
Foreign Address	Remote IPv6 address
State	IPv6 TCP connection status, including • Closed • Listening • Syn_Sent • Syn_Rcvd • Established • Close_Wait • Fin_Wait1 • Closing • Last_Ack • Fin_Wait2 • Time_Wait

display udp ipv6 statistics

Syntax

display udp ipv6 statistics [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display udp ipv6 statistics** command to display the statistics of IPv6 UDP packets.

You can use the **reset udp ipv6 statistics** command to clear the statistics of all IPv6 UDP packets.

Examples

Display the statistics information of IPv6 UDP packets.

```
<Sysname> display udp ipv6 statistics
Received packets:
     Total: 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
```

Table 41 Output description

Field	Description
Total	Total number of received/sent packets
checksum error	Total number of packets with a checksum error
shorter than header	Total number of IPv6 UDP packets whose total length is less than that specified by the packet header
data length larger than packet	Total number of packets whose data length exceeds that specified by the packet header
unicast(no socket on port)	Total number of received unicast packets without any socket
broadcast/multicast(no socket on port)	Total number of received broadcast/multicast packets without any socket
not delivered, input socket full	Number of packets not handled because of the receive buffer being full
input packet missing pcb cache	Number of packets failing to match the protocol control block (PCB) cache

ipv6

Syntax

ipv6

undo ipv6

View

System view

Default level

2: System level

Parameters

None

Description

Use the **ipv6** command to enable IPv6.

Use the **undo ipv6** command to disable IPv6.

By default, IPv6 is disabled.

Examples

Enable IPv6.

```
<Sysname> system-view
[Sysname] ipv6
```

ipv6 address

Syntax

ipv6 address { *ipv6-address prefix-length* | *ipv6-address/prefix-length* }

undo ipv6 address [*ipv6-address prefix-length* | *ipv6-address/prefix-length*]

View

Interface view

Default level

2: System level

Parameters

ipv6-address: IPv6 address.

prefix-length: Prefix length of the IPv6 address, in the range 1 to 128.

Description

Use the **ipv6 address** command to configure an IPv6 global unicast address for an interface.

Use the **undo ipv6 address** command to remove the IPv6 address from the interface.

By default, no global unicast address is configured for an interface.

Note that except the link-local address automatically obtained and the one generated through stateless autoconfiguration, all IPv6 addresses will be removed from the interface if you carry out the **undo ipv6 address** command without any parameter specified.

Examples

Set the global IPv6 unicast address of VLAN-interface 100 to 2001::1 with prefix length 64.

Method I:

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1/64
```

Method II:

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1 64
```

ipv6 address anycast

Syntax

ipv6 address *ipv6-address/prefix-length* **anycast**

undo ipv6 address *ipv6-address/prefix-length* **anycast**

View

Interface view

Default level

2: System level

Parameters

ipv6-address/prefix-length: Specifies an IPv6 anycast address and its prefix length. The prefix length ranges 1 to 128.

Description

Use the **ipv6 address anycast** command to configure an IPv6 anycast address for an interface.

Use the **undo ipv6 address anycast** command to remove the IPv6 anycast address from the interface.

By default, no IPv6 anycast address is configured for an interface.

Examples

Set the IPv6 anycast address of VLAN-interface 100 to 2001::1 with prefix length 64.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1/64 anycast
```

ipv6 address auto

Syntax

ipv6 address auto

undo ipv6 address auto

View

Interface view

Default level

2: System level

Parameters

None

Description

Use the **ipv6 address auto** command to enable the stateless address autoconfiguration function on the interface. With this function enabled, the interface can automatically generate a global unicast address.

Use the **undo ipv6 address auto** command to disable this function.

The stateless address autoconfiguration function is disabled by default.

NOTE:

After a global unicast address is generated through stateless autoconfiguration, a link-local address is generated automatically, which can be removed only by executing the **undo ipv6 address auto** command.

Examples

Enable stateless address autoconfiguration on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address auto
```

ipv6 address auto link-local

Syntax

ipv6 address auto link-local

undo ipv6 address auto link-local

View

Interface view

Default level

2: System level

Parameters

None

Description

Use the **ipv6 address auto link-local** command to automatically generate a link-local address for an interface.

Use the **undo ipv6 address auto link-local** command to remove the automatically generated link-local address for the interface.

By default, no link-local address is configured on an interface, but it will automatically be generated after a global IPv6 unicast address is configured for the interface.

- After an IPv6 global unicast address is configured for an interface, a link-local address is generated automatically. The automatically generated link-local address is the same as the one generated by using the **ipv6 address auto link-local** command.
- The **undo ipv6 address auto link-local** command can only remove the link-local addresses generated through the **ipv6 address auto link-local** command. After the **undo ipv6 address auto link-local** command is used on an interface that has an IPv6 global unicast address configured, the interface still has a link-local address. If the interface has no IPv6 global unicast address configured, it will have no link-local address.
- Manual assignment takes precedence over automatic generation. If you first adopt automatic generation and then manual assignment, the manually assigned link-local address will overwrite the automatically generated one. If you first adopt manual assignment and then automatic generation, the automatically generated link-local address will not take effect and the link-local address of an interface is still the manually assigned one. If you delete the manually assigned address, the automatically generated link-local address is validated. For more information about manually assignment of an IPv6 link-local address, see the **ipv6 address link-local** command.

Examples

Configure VLAN-interface 100 to automatically generate a link-local address.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address auto link-local
```

ipv6 address eui-64

Syntax

ipv6 address *ipv6-address/prefix-length* **eui-64**

undo ipv6 address *ipv6-address/prefix-length* **eui-64**

View

Interface view

Default level

2: System level

Parameters

ipv6-address/prefix-length: IPv6 address and IPv6 prefix. The *ipv6-address* and *prefix-length* arguments jointly specify the prefix of an EUI-64 IPv6 address.

Description

Use the **ipv6 address eui-64** command to configure an EUI-64 IPv6 address for an interface.

Use the **undo ipv6 address eui-64** command to remove the configured EUI-64 IPv6 address for the interface.

By default, no EUI-64 IPv6 address is configured for an interface.

An EUI-64 IPv6 address is generated based on the specified prefix and the automatically generated interface identifier and can be displayed by using the **display ipv6 interface** command.

Note that you cannot specify the prefix length of an EUI-64 IPv6 address to be greater than 64.

Examples

Configure an EUI-64 IPv6 address for VLAN-interface 100. The prefix length of the address is the same as that of 2001::1/64, and the interface ID is generated based on the MAC address of the device.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1/64 eui-64
```

ipv6 address link-local

Syntax

ipv6 address *ipv6-address* **link-local**

undo ipv6 address *ipv6-address* **link-local**

View

Interface view

Default level

2: System level

Parameters

ipv6-address: IPv6 link-local address. The first 10 bits of an address must be 1111111010 (binary). The first group of hexadecimals in the address must be FE80 to FEBF.

Description

Use the **ipv6 address link-local** command to configure a link-local address for the interface.

Use the **undo ipv6 address link-local** command to remove the configured link-local address for the interface.

Manual assignment takes precedence over automatic generation. If you first adopt automatic generation and then manual assignment, the manually assigned link-local address will overwrite the automatically generated one. If you first adopt manual assignment and then automatic generation, the automatically generated link-local address will not take effect and the link-local address of an interface is still the manually assigned one. If you delete the manually assigned address, the automatically generated link-local address is validated. For automatic generation of an IPv6 link-local address, see the **ipv6 address auto link-local** command.

Examples

Configure a link-local address for VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address fe80::1 link-local
```

ipv6 fibcache

Syntax

ipv6 fibcache { *slot-number* | **all** }

undo ipv6 fibcache { *slot-number* | **all** }

View

System view

Default level

2: System level

Parameters

slot-number: ID of an IRF member device. You can use the **display irf** command to view the IDs of IRF member devices. If no IRF is formed, the *slot-number* is the number of the current device.

all: Specifies all IRF member devices.

Description

Use the **ipv6 fibcache** command to enable the IPv6 FIB cache function.

Use the **undo ipv6 fibcache** command to disable the IPv6 FIB cache function.

By default, the IPv6 FIB cache function is disabled.

The IPv6 FIB cache function takes effect only on packets to be forwarded.

Examples

Enable the IPv6 FIB cache function.

```
<Sysname> system-view
[Sysname] ipv6 fibcache 1
```

ipv6 fib-loadbalance-type hash-based

Syntax

ipv6 fib-loadbalance-type hash-based

undo ipv6 fib-loadbalance-type hash-based

View

System view

Default level

2: System level

Parameters

None

Description

Use the **ipv6 fib-loadbalance-type hash-based** command to enable hash-based load sharing.

Use the **undo ipv6 fib-loadbalance-type hash-based** command to restore the default.

By default, polling-based load sharing is used, and equal-cost routes are used in turn to forward packets.

Examples

Enable hash-based load sharing.

```
<Sysname> system-view
[Sysname] ipv6 fib-loadbalance-type hash-based
```

ipv6 hoplimit-expires enable

Syntax

ipv6 hoplimit-expires enable

undo ipv6 hoplimit-expires

View

System view

Default level

2: System level

Parameters

None

Description

Use the **ipv6 hoplimit-expires enable** command to enable the sending of ICMPv6 Time Exceeded packets.

Use the **undo ipv6 hoplimit-expires** command to disable the sending of ICMPv6 Time Exceeded packets.

By default, the sending of ICMPv6 Time Exceeded packets is enabled.

After you disable the sending of ICMPv6 Time Exceeded packets, the switch will still send Fragment Reassembly Time Exceeded packets.

Examples

Disable the sending of ICMPv6 Time Exceeded packets.

```
<Sysname> system-view
[Sysname] undo ipv6 hoplimit-expires
```

ipv6 icmp-error

Syntax

ipv6 icmp-error { **bucket** *bucket-size* | **ratelimit** *interval* } *

undo ipv6 icmp-error

View

System view

Default level

2: System level

Parameters

bucket *bucket-size*: Number of tokens in the token bucket, in the range of 1 to 200.

ratelimit *interval*: Update period of the token bucket in milliseconds, in the range of 0 to 2,147,483,647. The update period "0" indicates that the number of ICMPv6 error packets sent is not restricted.

Description

Use the **ipv6 icmp-error** command to configure the size and update period of the token bucket.

Use the **undo ipv6 icmp-error** command to restore the defaults.

By default, the size is 10 and the update period is 100 milliseconds. At most 10 ICMPv6 error packets can be sent within 100 milliseconds.

Examples

Set the capacity of the token bucket to 50 and the update period to 100 milliseconds.

```
<Sysname> system-view
[Sysname] ipv6 icmp-error bucket 50 ratelimit 100
```

ipv6 icmpv6 multicast-echo-reply enable

Syntax

ipv6 icmpv6 multicast-echo-reply enable

undo ipv6 icmpv6 multicast-echo-reply

View

System view

Default level

2: System level

Parameters

None

Description

Use the **ipv6 icmpv6 multicast-echo-reply enable** command to enable replying to multicast echo requests.

Use the **undo ipv6 icmpv6 multicast-echo-reply** command to disable replying to multicast echo requests.

By default, the switch is disabled from replying to multicast echo requests.

Examples

Enable replying to multicast echo requests.

```
<Sysname> system-view
[Sysname] ipv6 icmpv6 multicast-echo-reply enable
```

ipv6 nd autoconfig managed-address-flag

Syntax

ipv6 nd autoconfig managed-address-flag

undo ipv6 nd autoconfig managed-address-flag

View

Interface view

Default level

2: System level

Parameters

None

Description

Use the **ipv6 nd autoconfig managed-address-flag** command to set the managed address configuration (M) flag to 1 so that the host can acquire an IPv6 address through stateful autoconfiguration (for example, from a DHCP server).

Use the **undo ipv6 nd autoconfig managed-address-flag** command to restore the default.

By default, the M flag is set to **0** so that the host can acquire an IPv6 address through stateless autoconfiguration.

Examples

Configure the host to acquire an IPv6 address through stateful autoconfiguration.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd autoconfig managed-address-flag
```

ipv6 nd autoconfig other-flag

Syntax

ipv6 nd autoconfig other-flag

undo ipv6 nd autoconfig other-flag

View

Interface view

Default level

2: System level

Parameters

None

Description

Use the **ipv6 nd autoconfig other-flag** command to set the other stateful configuration flag (O) to 1 so that the host can acquire information other than IPv6 address through stateful autoconfiguration (for example, from a DHCP server).

Use the **undo ipv6 nd autoconfig other-flag** command to restore the default.

By default, the O flag is set to **0** so that the host can acquire other information through stateless autoconfiguration.

Examples

Configure the host to acquire information other than IPv6 address through stateless autoconfiguration.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo ipv6 nd autoconfig other-flag
```

ipv6 nd dad attempts

Syntax

ipv6 nd dad attempts *value*

undo ipv6 nd dad attempts

View

Interface view

Default level

2: System level

Parameters

value: Number of attempts to send an NS message for DAD, in the range of 0 to 600. The default value is 1. When it is set to 0, DAD is disabled.

Description

Use the **ipv6 nd dad attempts** command to configure the number of attempts to send an NS message for DAD.

Use the **undo ipv6 nd dad attempts** command to restore the default.

By default, the number of attempts to send an NS message for DAD is 1.

Related commands: **display ipv6 interface**.

Examples

Set the number of attempts to send an NS message for DAD to 20.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd dad attempts 20
```

ipv6 nd hop-limit

Syntax

ipv6 nd hop-limit *value*

undo ipv6 nd hop-limit

View

System view

Default level

2: System level

Parameters

value: Number of hops, in the range of 0 to 255. When it is set to 0, the Hop Limit field in RA messages sent by the switch is 0. The number of hops is determined by the requesting device itself.

Description

Use the **ipv6 nd hop-limit** command to configure the hop limit advertised by the switch.

Use the **undo ipv6 nd hop-limit** command to restore the default hop limit.

By default, the hop limit advertised by the switch is 64.

Examples

Set the hop limit advertised by the switch to 100.

```
<Sysname> system-view
[Sysname] ipv6 nd hop-limit 100
```

ipv6 nd ns retrans-timer

Syntax

ipv6 nd ns retrans-timer *value*

undo ipv6 nd ns retrans-timer

View

Interface view

Default level

2: System level

Parameters

value: Interval for retransmitting an NS message in milliseconds, in the range of 1,000 to 4,294,967,295.

Description

Use the **ipv6 nd ns retrans-timer** command to set the interval for retransmitting an NS message. The local interface retransmits an NS message at intervals of this value. Furthermore, the Retrans Timer field in RA messages sent by the local interface is equal to this value.

Use the **undo ipv6 nd ns retrans-timer** command to restore the default.

By default, the local interface sends NS messages at 1000 millisecond intervals and the value of the Retrans Timer field in RA messages sent by the local interface is 0, so that the interval for retransmitting an NS message is determined by the receiving device.

Related commands: **display ipv6 interface**.

Examples

Specify VLAN-interface 100 to retransmit NS messages at intervals of 10,000 milliseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ns retrans-timer 10000
```

ipv6 nd nud reachable-time

Syntax

ipv6 nd nud reachable-time *value*

undo ipv6 nd nud reachable-time

View

Interface view

Default level

2: System level

Parameters

value: Neighbor reachable time in milliseconds, in the range of 1 to 3,600,000.

Description

Use the **ipv6 nd nud reachable-time** command to configure the neighbor reachable time on an interface. This time value serves as not only the neighbor reachable time on the local interface, but also the value of the Reachable Time field in RA messages sent by the local interface.

Use the **undo ipv6 nd nud reachable-time** command to restore the default.

By default, the neighbor reachable time on the local interface is 30,000 milliseconds and the value of the Reachable Time field in RA messages is 0, so that the reachable time is determined by the receiving device.

Related commands: **display ipv6 interface**.

Examples

Set the neighbor reachable time on VLAN-interface 100 to 10,000 milliseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd nud reachable-time 10000
```

ipv6 nd ra halt

Syntax

ipv6 nd ra halt

undo ipv6 nd ra halt

View

Interface view

Default level

2: System level

Parameters

None

Description

Use the **ipv6 nd ra halt** command to enable RA message suppression.

Use the **undo ipv6 nd ra halt** command to disable RA message suppression.

By default, RA messages are suppressed.

Examples

Suppress RA messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra halt
```

ipv6 nd ra interval

Syntax

ipv6 nd ra interval *max-interval-value min-interval-value*

undo ipv6 nd ra interval

View

Interface view

Default level

2: System level

Parameters

max-interval-value: Maximum interval for advertising RA messages in seconds, in the range of 4 to 1,800.

min-interval-value: Minimum interval for advertising RA messages in seconds, in the range of 3 to 1,350.

Description

Use the **ipv6 nd ra interval** command to set the maximum and minimum intervals for advertising RA messages. The device advertises RA messages at intervals of a random value between the maximum interval and the minimum interval.

Use the **undo ipv6 nd ra interval** command to restore the default.

By default, the maximum interval between RA messages is 600 seconds, and the minimum interval is 200 seconds.

NOTE:

- The minimum interval should be three-fourths of the maximum interval or less.
- The maximum interval for sending RA messages should be less than or equal to the router lifetime in RA messages.

Examples

Set the maximum interval for advertising RA messages to 1,000 seconds and the minimum interval to 700 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra interval 1000 700
```

ipv6 nd ra no-advlinkmtu

Syntax

ipv6 nd ra no-advlinkmtu

undo ipv6 nd ra no-advlinkmtu

View

Interface view

Default level

2: System level

Parameters

None

Description

Use the **ipv6 nd ra no-advlinkmtu** command to turn off the MTU option in RA messages.

Use the **undo ipv6 nd ra no-advlinkmtu** command to restore the default.

By default, RA messages contain the MTU option.

Examples

Turn off the MTU option in RA messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra no-advlinkmtu
```

ipv6 nd ra prefix

Syntax

ipv6 nd ra prefix { *ipv6-prefix prefix-length* | *ipv6-prefix/prefix-length* } *valid-lifetime preferred-lifetime* [**no-autoconfig** | **off-link**] *

undo ipv6 nd ra prefix *ipv6-prefix*

View

Interface view

Default level

2: System level

Parameters

prefix-length: Prefix length of the IPv6 address.

ipv6-prefix: IPv6 address prefix.

valid-lifetime: Valid lifetime of a prefix in seconds, in the range of 0 to 4,294,967,295.

preferred-lifetime: Preferred lifetime of a prefix used for stateless autoconfiguration in seconds, in the range of 0 to 4,294,967,295.

no-autoconfig: Specifies a prefix not to be used for stateless autoconfiguration. If this keyword is not provided, the prefix is used for stateless autoconfiguration.

off-link: Indicates that the address with the prefix is not directly reachable on the link. If this keyword is not provided, the address with the prefix is directly reachable on the link.

Description

Use the **ipv6 nd ra prefix** command to configure the prefix information in RA messages.

Use the **undo ipv6 nd ra prefix** command to remove the prefix information from RA messages.

By default, no prefix information is configured in RA messages and the IPv6 address of the interface sending RA messages is used as the prefix information with valid lifetime 2592000 seconds (that is, 30 days) and preferred lifetime 604800 seconds (that is, 7 days).

Examples

Configure the prefix information for RA messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra prefix 2001:10::100/64 100 10
```

ipv6 nd ra router-lifetime

Syntax

ipv6 nd ra router-lifetime *value*

undo ipv6 nd ra router-lifetime

View

Interface view

Default level

2: System level

Parameters

value: Router lifetime in seconds, in the range of 0 to 9,000. When it is set to 0, the switch does not serve as the default router.

Description

Use the **ipv6 nd ra router-lifetime** command to configure the router lifetime in RA messages.

Use the **undo ipv6 nd ra router-lifetime** command to restore the default.

By default, the router lifetime in RA messages is 1,800 seconds.

Note that the router lifetime in RA messages should be greater than or equal to the advertising interval.

Examples

Set the router lifetime in RA messages on VLAN-interface 100 to 1,000 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra router-lifetime 1000
```

ipv6 nd snooping enable

Syntax

ipv6 nd snooping enable

undo ipv6 nd snooping enable

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use the **ipv6 nd snooping enable** command to enable ND snooping.

Use the **undo ipv6 nd snooping enable** command to restore the default.

By default, ND snooping is disabled.

Examples

Enable ND snooping for VLAN 1.

```
<Sysname> system-view
[Sysname] vlan 1
[Sysname-vlan1] ipv6 nd snooping enable
```

ipv6 nd snooping enable global

Syntax

ipv6 nd snooping enable global

undo ipv6 nd snooping enable global

View

System view

Default level

2: System level

Parameters

None

Description

Use the **ipv6 nd snooping enable global** command to enable ND snooping based on global unicast addresses (the devices use DAD NS messages containing global unicast addresses to create ND snooping entries)

Use the **undo ipv6 nd snooping enable global** command to restore the default.

By default, ND snooping based on global unicast addresses is disabled.

Examples

Enable ND snooping based on global unicast addresses.

```
<Sysname> system-view
[Sysname] ipv6 nd snooping enable global
```

ipv6 nd snooping enable link-local

Syntax

ipv6 nd snooping enable link-local

undo ipv6 nd snooping enable link-local

View

System view

Default level

2: System level

Parameters

None

Description

Use the **ipv6 nd snooping enable link-local** command to enable ND snooping based on link local addresses (the devices use DAD NS messages containing link local addresses to create ND snooping entries).

Use the **undo ipv6 nd snooping enable link-local** command to restore the default.

By default, ND snooping based on link local addresses is disabled.

Examples

Enable ND snooping based on link local addresses.

```
<Sysname> system-view
[Sysname] ipv6 nd snooping enable link-local
```

ipv6 nd snooping max-learning-num

Syntax

ipv6 nd snooping max-learning-num *number*

undo ipv6 nd snooping max-learning-num

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

number: Maximum number of ND snooping entries that can be learned by the interface, in the range of 0 to 1024.

Description

Use the **ipv6 nd snooping max-learning-num** command to configure the maximum number of ND snooping entries that can be learned on the interface.

Use the **undo ipv6 nd snooping max-learning-num** command to restore the default.

By default, the number of ND snooping entries that an interface can learn is not limited.

Examples

Set the maximum number of ND snooping entries that can be learned on Layer 2 Ethernet interface GigabitEthernet 1/0/1 to 1000.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd snooping max-learning-num 1000
```

Set the maximum number of ND snooping entries that can be learned on Layer 2 aggregate interface 1 to 1000.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] ipv6 nd snooping max-learning-num 1000
```

ipv6 nd snooping uplink

Syntax

ipv6 nd snooping uplink

undo ipv6 nd snooping uplink

View

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

None

Description

Use the **ipv6 nd snooping uplink** command to configure an interface as uplink interface, and disable the interface from learning ND snooping entries.

Use the **undo ipv6 nd snooping uplink** command to restore the default.

By default, with ND snooping enabled, the interface is allowed to learn ND snooping entries.

Examples

Configure Layer 2 Ethernet interface GigabitEthernet 1/0/1 as uplink interface, and disable the interface from learning ND snooping entries.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd snooping uplink
```

Configure Layer 2 aggregate interface Bridge-Aggregation 1 as uplink interface, and disable the interface from learning ND snooping entries.

```
<Sysname> system-view
[Sysname] interface Bridge-Aggregation 1
[Sysname-Bridge-Aggregation1] ipv6 nd snooping uplink
```

ipv6 neighbor

Syntax

ipv6 neighbor *ipv6-address mac-address* { *vlan-id port-type port-number* | **interface** *interface-type interface-number* }

undo ipv6 neighbor *ipv6-address interface-type interface-number*

View

System view

Default level

2: System level

Parameters

ipv6-address: IPv6 address of the static neighbor entry.

mac-address: MAC address of the static neighbor entry (48 bits long, in the format of H-H-H).

vlan-id: VLAN ID of the static neighbor entry, in the range of 1 to 4094.

port-type port-number: Type and number of a Layer 2 port of the static neighbor entry.

interface *interface-type interface-number*: Type and number of a Layer 3 interface of the static neighbor entry.

Description

Use the **ipv6 neighbor** command to configure a static neighbor entry.

Use the **undo ipv6 neighbor** command to remove a static neighbor entry.

You can use a Layer 3 VLAN interface or a Layer 2 port in the VLAN to configure a static neighbor entry.

- If the first method is used, the neighbor entry is in the INCMP state. After the switch obtains the corresponding Layer 2 port information through resolution, the neighbor entry will go into the REACH state.
- If the second method is used, the corresponding VLAN interface must exist and the port specified by *port-type port-number* must belong to the VLAN specified by *vlan-id*. After the static neighbor entry is configured, the switch will relate the VLAN interface with the IPv6 address to identify the static neighbor entry uniquely and the entry will be in the REACH state.

To remove such a static neighbor entry, you only need to specify the corresponding VLAN interface and the neighbor address.

Related commands: **display ipv6 neighbors**.

Examples

Configure a static neighbor entry for Layer 2 port GigabitEthernet 1/0/1 of VLAN 100.

```
<Sysname> system-view
[Sysname] ipv6 neighbor 2000::1 fe-e0-89 100 GigabitEthernet 1/0/1
```

ipv6 neighbors max-learning-num

Syntax

ipv6 neighbors max-learning-num *number*

undo ipv6 neighbors max-learning-num

View

Interface view

Default level

2: System level

Parameters

number: Maximum number of neighbors that can be dynamically learned by the interface, in the range of 1 to 256.

Description

Use the **ipv6 neighbors max-learning-num** command to configure the maximum number of neighbors that can be dynamically learned on the interface.

Use the **undo ipv6 neighbors max-learning-num** command to restore the default.

By default, the maximum number of neighbors that can be dynamically learned on the interface is 256.

Examples

Set the maximum number of neighbors that can be dynamically learned on VLAN-interface 100 to 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 neighbors max-learning-num 10
```

ipv6 pathmtu

Syntax

ipv6 pathmtu *ipv6-address* [*value*]

undo ipv6 pathmtu *ipv6-address*

View

System view

Default level

2: System level

Parameters

ipv6-address: IPv6 address.

value: PMTU of a specified IPv6 address in bytes, in the range of 1280 to 10000.

Description

Use the **ipv6 pathmtu** command to configure a static PMTU for a specified IPv6 address.

Use the **undo ipv6 pathmtu** command to remove the PMTU configuration for a specified IPv6 address.

By default, no static PMTU is configured.

Examples

Configure a static PMTU for a specified IPv6 address.

```
<Sysname> system-view
[Sysname] ipv6 pathmtu fe80::12 1300
```

ipv6 pathmtu age

Syntax

ipv6 pathmtu age *age-time*

undo ipv6 pathmtu age

View

System view

Default level

2: System level

Parameters

age-time: Aging time for PMTU in minutes, in the range of 10 to 100.

Description

Use the **ipv6 pathmtu age** command to configure the aging time for a dynamic PMTU.

Use the **undo ipv6 pathmtu age** command to restore the default.

By default, the aging time is 10 minutes.

Note that the aging time is invalid for a static PMTU.

Related commands: **display ipv6 pathmtu**.

Examples

Set the aging time for a dynamic PMTU to 40 minutes.

```
<Sysname> system-view
[Sysname] ipv6 pathmtu age 40
```

ipv6 unreachables enable

Syntax

ipv6 unreachables enable

undo ipv6 unreachables

View

System view

Default level

2: System level

Parameters

None

Description

Use the **ipv6 unreachables enable** command to enable sending of ICMPv6 destination unreachable packets.

Use the **undo ipv6 unreachables** command to disable sending of ICMPv6 destination unreachable packets.

By default, sending of ICMPv6 destination unreachable packets is disabled.

Examples

Enable sending of ICMPv6 destination unreachable packets.

```
<Sysname> system-view
[Sysname] ipv6 unreachables enable
```

reset ipv6 fibcache

Syntax

reset ipv6 fibcache { *slot-number* | **all** }

View

User view

Default level

2: System level

Parameters

slot-number: ID of an IRF member device. You can use the **display irf** command to view the IDs of IRF member devices. If no IRF is formed, the *slot-number* is the number of the current device.

all: Specifies all IRF member devices.

Description

Use the **ipv6 fibcache** command to clear the IPv6 FIB cache of the specified device.

Examples

Clear the IPv6 FIB cache of the specified device.

```
<Sysname> system-view
[Sysname] reset fibcache 1
```

reset ipv6 nd snooping

Syntax

reset ipv6 nd snooping [*ipv6-address* | **vlan** *vlan-id*]

View

User view

Default level

2: System level

Parameters

ipv6-address: Clears the ND snooping entries of the specified IPv6 address.

vlan *vlan-id*: Clears the ND snooping entries of the specified VLAN. The VLAN ID ranges 1 to 4094.

Description

Use the **reset ipv6 nd snooping** command to clear ND snooping entries.

If no parameter is specified, this command clears all ND snooping entries.

Examples

Clear all ND snooping entries on VLAN 1.

```
<Sysname> reset ipv6 nd snooping vlan 1
```

reset ipv6 neighbors

Syntax

reset ipv6 neighbors { **all** | **dynamic** | **interface** *interface-type interface-number* | **slot** *slot-number* | **static** }

View

User view

Default level

2: System level

Parameters

all: Clears static and dynamic neighbor information on all interfaces.

dynamic: Clears dynamic neighbor information on all interfaces.

interface *interface-type interface-number*: Clears dynamic neighbor information on a specified interface.

slot *slot-number*: Clears dynamic neighbor information on a specified device in an IRF. If no IRF is formed, only the dynamic neighbor information of the current device is cleared. The *slot-number* argument indicates the member ID of the device.

static: Clears static neighbor information on all interfaces.

Description

Use the **reset ipv6 neighbors** command to clear IPv6 neighbor information.

You can use the **display ipv6 neighbors** command to display the current IPv6 neighbor information.

Examples

Clear neighbor information on all interfaces.

```
<Sysname> reset ipv6 neighbors all
```

Clear dynamic neighbor information on all interfaces.

```
<Sysname> reset ipv6 neighbors dynamic
```

Clear all neighbor information on VLAN-interface 1.

```
<Sysname> reset ipv6 neighbors interface GigabitEthernet 1/0/1
```

reset ipv6 pathmtu

Syntax

reset ipv6 pathmtu { **all** | **static** | **dynamic** }

View

User view

Default level

2: System level

Parameters

all: Clears all PMTUs.

static: Clears all static PMTUs.

dynamic: Clears all dynamic PMTUs.

Description

Use the **reset ipv6 pathmtu** the command to clear the PMTU information.

Examples

Clear all PMTUs.

```
<Sysname> reset ipv6 pathmtu all
```

reset ipv6 statistics

Syntax

reset ipv6 statistics [**slot** *slot-number*]

View

User view

Default level

2: System level

Parameters

slot *slot-number*: Clears the statistics of IPv6 packets and ICMPv6 packets on a specified device in an IRF. If no IRF is formed, related information on the current device is cleared only. The *slot-number* argument indicates the member ID of the device.

Description

Use the **reset ipv6 statistics** command to clear the statistics of IPv6 packets and ICMPv6 packets.

You can use the **display ipv6 statistics** command to display the statistics of IPv6 and ICMPv6 packets.

Examples

Clear the statistics of IPv6 packets and ICMPv6 packets.

```
<Sysname> reset ipv6 statistics
```

reset tcp ipv6 statistics

Syntax

reset tcp ipv6 statistics

View

User view

Default level

2: System level

Parameters

None

Description

Use the **reset tcp ipv6 statistics** command to clear the statistics of all IPv6 TCP connections.

You can use the **display tcp ipv6 statistics** command to display the statistics of IPv6 TCP connections.

Examples

Clear the statistics of all IPv6 TCP connections.

```
<Sysname> reset tcp ipv6 statistics
```

reset udp ipv6 statistics

Syntax

reset udp ipv6 statistics

View

User view

Default level

2: System level

Parameters

None

Description

Use the **reset udp ipv6 statistics** command to clear the statistics of all IPv6 UDP packets.

You can use the **display udp ipv6 statistics** command to display the statistics of IPv6 UDP packets.

Examples

Clear the statistics of all IPv6 UDP packets.

```
<Sysname> reset udp ipv6 statistics
```

tcp ipv6 timer fin-timeout

Syntax

tcp ipv6 timer fin-timeout *wait-time*

undo tcp ipv6 timer fin-timeout

View

System view

Default level

2: System level

Parameters

wait-time: Length of the finwait timer for IPv6 TCP connections in seconds, in the range of 76 to 3,600.

Description

Use the **tcp ipv6 timer fin-timeout** command to set the finwait timer for IPv6 TCP connections.

Use the **undo tcp ipv6 timer fin-timeout** command to restore the default.

By default, the length of the finwait timer is 675 seconds.

Examples

Set the finwait timer length of IPv6 TCP connections to 800 seconds.

```
<Sysname> system-view
[Sysname] tcp ipv6 timer fin-timeout 800
```

tcp ipv6 timer syn-timeout

Syntax

tcp ipv6 timer syn-timeout *wait-time*

undo tcp ipv6 timer syn-timeout

View

System view

Default level

2: System level

Parameters

wait-time: Length of the synwait timer for IPv6 TCP connections in seconds, in the range of 2 to 600.

Description

Use the **tcp ipv6 timer syn-timeout** command to set the synwait timer for IPv6 TCP connections

Use the **undo tcp ipv6 timer syn-timeout** command to restore the default.

By default, the length of the synwait timer of IPv6 TCP connections is 75 seconds.

Examples

Set the synwait timer length of IPv6 TCP connections to 100 seconds.

```
<Sysname> system-view
[Sysname] tcp ipv6 timer syn-timeout 100
```

tcp ipv6 window

Syntax

tcp ipv6 window *size*

undo tcp ipv6 window

View

System view

Default level

2: System level

Parameters

size: Size of the IPv6 TCP send/receive buffer in KB (kilobyte), in the range of 1 to 32.

Description

Use the **tcp ipv6 window** command to set the size of the IPv6 TCP send/receive buffer.

Use the **undo tcp ipv6 window** command to restore the default.

By default, the size of the IPv6 TCP send/receive buffer is 8 KB.

Examples

Set the size of the IPv6 TCP send/receive buffer to 4 KB.

```
<Sysname> system-view
[Sysname] tcp ipv6 window 4
```

DHCPv6 configuration commands

DHCPv6 common configuration commands

display ipv6 dhcp duid

Syntax

display ipv6 dhcp duid [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display ipv6 dhcp duid** command to display the DUID of the local device.

Examples

Display the DUID of the device.

```
<Sysname> display ipv6 dhcp duid
The DUID of this device: 0003-0001-00e0-fc00-5552
```

DHCPv6 server configuration commands

display ipv6 dhcp pool

Syntax

display ipv6 dhcp pool [*pool-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

pool-number: Displays the details about the address pool specified by the pool number. The value ranges from 1 to 128.. If no pool number is specified, all address pool information is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display ipv6 dhcp pool** command to display DHCPv6 address pool information.

Examples

Display all address pool information.

```
<Sysname> display ipv6 dhcp pool
Pool            Prefix-pool
1               1
2               Not configured
```

Table 42 Output description

Field	Description
Pool	DHCPv6 address pool number
Prefix-pool	Prefix pool referenced by the address pool. If no referenced prefix pool is specified, this field displays "Not configured".

Display detailed information about a specified address pool.

```
<Sysname> display ipv6 dhcp pool 1
DHCPv6 pool: 1
  Static bindings:
    DUID: 0003000100E0FC000001
    IAID: 0000003F
    Prefix: 2::/64
      preferred lifetime 604800, valid lifetime 2592000
  Prefix pool: 1
    preferred lifetime 201600, valid lifetime 864000
  DNS server address:
    2::2
    2::3
  Domain name: aaa.com
  SIP server address:
    5::1
  SIP server domain name:
    bbb.com
```

Table 43 Output description

Field	Description
DHCPv6 pool	DHCPv6 address pool number
Static bindings	Static prefix information configured in the address pool. If no static prefix is configured, this field is not displayed.
DUID	Client DUID
IAID	Client IAID. If the IAID is not configured, this field displays "Not configured".
Prefix	IPv6 address prefix
preferred lifetime	Preferred lifetime of the prefix, in seconds
valid lifetime	Valid lifetime of the prefix, in seconds
Prefix Pool	Prefix pool referenced by the address pool. If no prefix pool is referenced, this field is not displayed.
DNS server address	DNS server address. If no DNS server address is configured, this field is not displayed.
Domain name	Domain name. If no domain name is configured, this field is not displayed.
SIP server address	SIP server address. If no SIP server address is configured, this field is not displayed.
SIP server domain name	Domain name of the SIP server. If no domain name of the SIP server is configured, this field is not displayed.

display ipv6 dhcp prefix-pool

Syntax

display ipv6 dhcp prefix-pool [*prefix-pool-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

prefix-pool-number: Displays details about the prefix pool specified by the prefix pool number. The value ranges from 1 to 128.. If no prefix pool number is specified, the brief information of all prefix pools is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display ipv6 dhcp prefix-pool** command to display prefix pool information.

Examples

Display brief information about all prefix pools.

```
<Sysname> display ipv6 dhcp prefix-pool
Prefix-pool Prefix                                  Available In-use Static
1           5::/64                                  64        0      0
```

Display details about the specified prefix pool.

```
<Sysname> display ipv6 dhcp prefix-pool 1
Prefix: 5::/64
Assigned length: 70
Total prefix number: 64
Available: 64
In-use: 0
Static: 0
```

Table 44 Output description

Field	Description
Prefix-pool	Prefix pool number
Prefix	Prefix contained in the prefix pool
Available	Number of idle prefixes
In-use	Number of assigned prefixes
Static	Number of static prefixes
Assigned length	Length of prefixes to be assigned
Total prefix number	Total number of prefixes

display ipv6 dhcp server

Syntax

display ipv6 dhcp server [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface *interface-type interface-number*: Displays the DHCPv6 server information of the interface specified by interface type and number. If no interface is specified, the DHCPv6 server information of all interfaces is displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display ipv6 dhcp server** command to display DHCPv6 server information.

Examples

Display the DHCPv6 server information of all interfaces.

```
<Sysname> display ipv6 dhcp server
DHCPv6 server status: Enabled
Interface             Pool
Vlan-interface2       1
Vlan-interface3       2
```

Display the DHCPv6 server information on the specified interface.

```
<Sysname> display ipv6 dhcp server interface vlan-interface 2
Using pool: 1
Preference value: 0
Allow-hint: Enabled
Rapid-commit: Disabled
```

Table 45 Output description

Field	Description
DHCPv6 server status	DHCPv6 server status, which can be "Enabled" or "Disabled".
Interface	Interface on which the DHCPv6 server is enabled
Pool	Address pool applied to the interface
Using pool	Address pool applied to the interface
Preference value	Server priority in the DHCPv6 Advertise message. The value ranges from 0 to 255.
Allow-hint	Support for desired prefix assignment. The status can be "Enabled" or "Disabled."
Rapid-commit	Support for rapid prefix assignment. The status can be "Enabled" or "Disabled."

display ipv6 dhcp server pd-in-use

Syntax

display ipv6 dhcp server pd-in-use { **all** | **pool** *pool-number* | **prefix** *prefix/prefix-len* | **prefix-pool** *prefix-pool-number* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

all: Displays all PD information.

pool *pool-number*: Displays the PD information of the address pool specified by the pool number. The value ranges from 1 to 128..

prefix *prefix/prefix-len*: Displays the PD information of the specified prefix. The *prefix/prefix-len* indicates the IPv6 prefix and prefix length. The value of the prefix length ranges from 1 to 128.

prefix-pool *prefix-pool-number*: Displays the PD information of the prefix pool specified by the prefix pool number. The value range of the prefix pool number depends on the device model.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display ipv6 dhcp server pd-in-use** command to display PD information.

Note that the PD information generated for static prefixes is not displayed when you display the PD information of a specific prefix pool.

Examples

Display all PD information.

```
<Sysname> display ipv6 dhcp server pd-in-use all
Total number = 3
Prefix                                  Type      Pool Lease-expiration
2:1::/24                                Auto(O)   1    Jul 10 2008 19:45:01
1:1::/64                                Static(F) 2    Not available
1:2::/64                                Static(O) 3    Oct  9 2008 09:23:31
```

Display the PD information of the specified address pool.

```
<Sysname> display ipv6 dhcp server pd-in-use pool 1
Total number = 2
Prefix                                  Type      Pool Lease-expiration
2:1::/24                                Auto(O)   1    Jul 10 2008 22:22:22
3:1::/64                                Static(C) 1    Jan  1 2008 11:11:11
```

Display the PD information of the specified prefix pool.

```
<Sysname> display ipv6 dhcp server pd-in-use prefix-pool 1
Total number = 1
Prefix                                  Type      Pool Lease-expiration
2:1:1:2::/64                            Auto(C)   2    Jan  1 2008 14:45:56
```

Display the PD information of the specified prefix.

```
<Sysname> display ipv6 dhcp server pd-in-use prefix 2:1::3/24
Pool: 1
Prefix pool: 1
Client: FE80::C800:CFF:FE18:0
Type: Auto(O)
DUID: 00030001CA000C180000
IAID: 0x00030001
```

```
Prefix: 2:1::/24
Preferred lifetime 400, valid lifetime 500
expires at Jul 10 2008 09:45:01 (288 seconds left)
```

Table 46 Output description

Field	Description
Total number	Total number of PDs
Prefix	Assigned IPv6 prefix
Type	PD type, which can be: • Static(F): Generated for the static prefix that has not been assigned to the client, and is also called the ineffective static PD. • Static(O): Temporarily generated for the static prefix to be assigned when the server receives a Solicit message from the corresponding client. • Static(C): Generated for the static prefix that is officially assigned. • Auto(O): Temporarily generated for the prefix selected from a prefix pool after the server receives a Solicit message from the client. • Auto(C): Generated for the prefix to be assigned officially after the server receives a Request message, or the server supporting rapid assignment receives the Solicit message containing a Rapid Commit option.
Pool	Address pool to which the PD belongs
Lease-expiration	Lease expiration time. If the lease will expire after the year 2100, this field displays "after 2100." For the ineffective static PD, this field displays "Not available."
Prefix Pool	Prefix pool to which the PD belongs. For the static PD, this field displays null.
Client	IPv6 address of the DHCPv6 client. For the ineffective static PD, this field displays null.
DUID	Client DUID
IAID	Client IAID. For the ineffective static PD with no IAID configured, this field displays null.
preferred lifetime	Preferred lifetime of the prefix, in seconds.
valid lifetime	Valid lifetime of the prefix, in seconds.
expires at	Lease expiration time. If the lease will expire after the year 2100, this field displays "expires after 2100."

display ipv6 dhcp server statistics

Syntax

display ipv6 dhcp server statistics [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display ipv6 dhcp server statistics** command to display packet statistics on the DHCPv6 server.

Examples

Display packet statistics on the DHCPv6 server.

```
<Sysname> display ipv6 dhcp server statistics
Packets received     :  0
  SOLICIT            :  0
  REQUEST            :  0
  CONFIRM            :  0
  RENEW              :  0
  REBIND             :  0
  RELEASE            :  0
  DECLINE            :  0
  INFORMATION-REQUEST:  0
  RELAY-FORWARD      :  0
Packets dropped      :  0
Packets sent         :  0
  ADVERTISE          :  0
  RECONFIGURE        :  0
  REPLY              :  0
  RELAY-REPLY        :  0
```

Table 47 Output description

Field	Description
Packets received	Number of messages received by the DHCPv6 server. The message types include: • SOLICIT • REQUEST • CONFIRM • RENEW • REBIND • RELEASE • DECLINE • INFORMATION-REQUEST • RELAY-FORWARD
Packets dropped	Number of packets discarded

Field	Description
Packets sent	Number of messages sent out from the DHCPv6 server. The message types include: • ADVERTISE • RECONFIGURE • REPLY • RELAY-REPLY

dns-server

Syntax

dns-server *ipv6-address*

undo dns-server *ipv6-address*

View

DHCPv6 address pool view

Default level

2: System level

Parameters

ipv6-address: IPv6 address of a DNS server.

Description

Use the **dns-server** command to specify a DNS server for the client.

Use the **undo dns-server** command to remove the specified DNS server.

No DNS server address is specified by default.

Note that:

- You can configure multiple DNS server addresses by using the **dns-server** command repeatedly.
- You can configure up to eight DNS servers in an address pool.
- The precedence of the specified DNS servers depends on the configuration sequence. The formerly specified DNS server takes precedence over the latter one.

Examples

Specify the DNS server address to be assigned to the client as 2:2::3.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] dns-server 2:2::3
```

domain-name

Syntax

domain-name *domain-name*

undo domain-name

View

DHCPv6 address pool view

Default level

2: System level

Parameters

domain-name: Domain name, a string of 1 to 50 characters.

Description

Use the **domain-name** command to configure the domain name for the client.

Use the **undo domain-name** command to remove the configuration.

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

You can configure only one domain name in an address pool.

If you repeatedly use the **domain-name** command, the latest configuration will overwrite the previous one.

Examples

Configure the domain name to be assigned to the client as aaa.com.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] domain-name aaa.com
```

ipv6 dhcp pool

Syntax

ipv6 dhcp pool *pool-number*

undo ipv6 dhcp pool *pool-number*

View

System view

Default level

2: System level

Parameters

pool-number: Address pool number. The value ranges from 1 to 128.

Description

Use the **ipv6 dhcp pool** command to create a DHCPv6 address pool and enter DHCPv6 address pool view, or enter DHCPv6 address pool view if the specified address pool already exists.

Use the **undo ipv6 dhcp pool** command to remove the address pool.

No DHCPv6 address pool is configured by default.

Examples

Create DHCPv6 address pool 1 and enter its view.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1]
```

ipv6 dhcp prefix-pool

Syntax

ipv6 dhcp prefix-pool *prefix-pool-number* **prefix** *prefix/prefix-len* **assign-len** *assign-len*

undo ipv6 dhcp prefix-pool *prefix-pool-number*

View

System view

Default level

2: System level

Parameters

prefix-pool-number: Prefix pool number. The value ranges from 1 to 128.

prefix *prefix/prefix-len*: Specifies the prefix contained in the specified prefix pool. The *prefix* indicates the IPv6 prefix. The *prefix-len* indicates the prefix length, in the range of 1 to 128.

assign-len *assign-len*: Specifies the length of the prefix assigned. The value ranges from 1 to 128. The *assign-len* must be higher than or equal to the *prefix-len*, and the difference between them must be less than or equal to 16.

Description

Use the **ipv6 dhcp prefix-pool** command to create a prefix pool and specify the prefix and the length of the prefix assigned.

Use the **undo ipv6 dhcp prefix-pool** command to remove the prefix pool.

No prefix pool is configured by default.

The prefix ranges of the prefix pools cannot overlap.

You cannot modify an existing prefix pool.

Removing a prefix pool will clear all PDs assigned from the prefix pool.

Examples

Create prefix pool 1 that contains the prefix 2001:0410::/32 and specify the length of prefixes to be assigned as 42. Prefix pool 1 can assign 1024 prefixes in the range of 2001:0410::/42 to 2001:0410:FFC0::/42.

```
<Sysname> system-view
[Sysname] ipv6 dhcp prefix-pool 1 prefix 2001:0410::/32 assign-len 42
```

ipv6 dhcp server apply pool

Syntax

ipv6 dhcp server apply pool *pool-number* [**allow-hint** | **preference** *preference-value* | **rapid-commit**] *

undo ipv6 dhcp server apply pool

View

Interface view

Default level

2: System level

Parameters

pool-number: Address pool number. The value ranges from 1 to 128.

allow-hint: Configure the server to support desired prefix assignment. If this keyword is not specified, the server does not support assignment of desired prefixes.

preference *preference-value*: Specifies the server priority in Advertise messages, in the range of 0 to 255. The default value is 0. A higher value indicates a higher priority.

rapid-commit: Configure the server to support rapid prefix assignment. If this keyword is not specified, the server does not support rapid prefix assignment.

Description

Use the **ipv6 dhcp server apply pool** command to apply a DHCPv6 address pool to the interface.

Use the **undo ipv6 dhcp server apply pool** command to remove the configuration.

No address pool is applied to an interface by default.

Upon receiving a request from a DHCPv6 client on an interface, the DHCPv6 server selects a prefix from the address pool applied to the interface and assigns it to the client.

With the **allow-hint** keyword specified, the server assigns the desired prefix to the requesting client. If the desired prefix is not included in the assignable prefix pool of the interface, or is already assigned to another client, the server ignores the desired prefix and assigns the client a prefix from the idle prefixes.

An interface cannot serve as a DHCPv6 server and DHCPv6 relay agent at the same time. It is not recommended that you enable the DHCPv6 server and DHCPv6 client on the same interface.

Only one address pool can be applied to an interface.

You can apply a non-existing address pool to an interface. However, the server cannot assign any prefix or other configuration information from the address pool until the address pool is created.

You cannot modify the address pool applied to an interface or parameters such as the server priority by using the **ipv6 dhcp server apply pool** command. You need to remove the applied address pool before you can apply another address pool to the interface or modify parameters such as the server priority.

Examples

Apply prefix pool 1 to VLAN-interface 2, configure the server to support desired prefix assignment and rapid prefix assignment, and set the highest priority of 255.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 dhcp server apply pool 1 allow-hint preference 255
rapid-commit
```

ipv6 dhcp server enable

Syntax

ipv6 dhcp server enable

undo ipv6 dhcp server enable

View

System view

Default level

2: System level

Parameters

None

Description

Use the **ipv6 dhcp server enable** command to enable the DHCPv6 server.

Use the **undo ipv6 dhcp server enable** command to disable the DHCPv6 server.

By default, the DHCPv6 server is disabled.

Note that other DHCPv6 server related configuration is effective only when the DHCPv6 server is enabled.

Examples

Enable the DHCPv6 server.

```
<Sysname> system-view
[Sysname] ipv6 dhcp server enable
```

prefix-pool

Syntax

prefix-pool *prefix-pool-number* [**preferred-lifetime** *preferred-lifetime* **valid-lifetime** *valid-lifetime*]

undo prefix-pool

View

DHCPv6 address pool view

Default level

2: System level

Parameters

prefix-pool-number: Prefix pool number. The value ranges from 1 to 128.

preferred-lifetime *preferred-lifetime*: Specifies the preferred lifetime of prefixes to be assigned. The value ranges from 60 to 4294967295, in seconds. The default value is 604800 seconds, that is, seven days.

valid-lifetime *valid-lifetime*: Specifies the valid lifetime of the prefixes to be assigned. The value ranges from 60 to 4294967295, in seconds. The default value is 2592000 seconds, that is, 30 days. The valid lifetime must be greater than or equal to the preferred lifetime.

Description

Use the **prefix-pool** command to apply a prefix pool to the DHCPv6 address pool, so that the DHCPv6 server can dynamically select a prefix from the prefix pool and assign it to the client.

Use the **undo prefix-pool** command to remove the configuration.

No prefix pool is referenced by an address pool by default.

Only one prefix pool can be referenced by an address pool.

A non-existing prefix pool can be referenced by an address pool. However, no prefix is available in the prefix pool for dynamic prefix assignment until the prefix pool is created.

You cannot modify the prefix pool referenced by an address pool, or the preferred lifetime or valid lifetime by using the **prefix-pool** command. You need to remove the configuration before you can have another prefix pool referenced by the address pool, or modify the preferred lifetime and valid lifetime.

Examples

Apply prefix pool 1 to address pool 1, and use the default preferred lifetime and valid lifetime.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] prefix-pool 1
```

Apply prefix pool 1 to address pool 1, and set the valid lifetime to three days, the preferred lifetime to one day.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] prefix-pool 1 preferred-lifetime 86400 valid-lifetime 259200
```

reset ipv6 dhcp server pd-in-use

Syntax

reset ipv6 dhcp server pd-in-use { **all** | **pool** *pool-number* | **prefix** *prefix/prefix-len* }

View

User view

Default level

1: Monitor level

Parameters

all: Clears all the PD information.

pool *pool-number*: Clears the PD information of the address pool specified by the pool number. The value ranges from 1 to 128.

prefix *prefix/prefix-len*: Clears the PD information of the specified prefix. The *prefix/prefix-len* indicates the IPv6 prefix and prefix length. The value of the prefix length ranges from 1 to 128.

Description

Use the **reset ipv6 dhcp server pd-in-use** command to clear the PD information of the DHCPv6 server.

Note that after the PD information of assigned static prefixes is removed, the PDs become ineffective static PDs.

Examples

Clear all the PD information.

```
<Sysname> reset ipv6 dhcp server pd-in-use all
```

Clear the PD information of the specified address pool.

```
<Sysname> reset ipv6 dhcp server pd-in-use pool 1
```

Clear the PD information of the specified prefix.

```
<Sysname> reset ipv6 dhcp server pd-in-use prefix 2001:0:0:1::/64
```

reset ipv6 dhcp server statistics

Syntax

reset ipv6 dhcp server statistics

View

User view

Default level

1: Monitor level

Parameters

None

Description

Use the **reset ipv6 dhcp server statistics** command to remove packet statistics on the DHCPv6 server.

Examples

Clear packet statistics on the DHCPv6 server.

```
<Sysname> reset ipv6 dhcp server statistics
```

sip-server

Syntax

sip-server { **address** *ipv6-address* | **domain-name** *domain-name* }

undo sip-server { **address** *ipv6-address* | **domain-name** *domain-name* }

View

DHCPv6 address pool view

Default level

2: System level

Parameters

address *ipv6-address*: Specifies the IPv6 address of a SIP server.

domain-name *domain-name*: Specifies the domain name of a SIP server. The domain name is a string of 1 to 50 characters.

Description

Use the **sip-server** command to configure the IPv6 address or domain name of a SIP server for the client.

Use the **undo sip-server** command to remove the configuration.

No SIP server address or domain name is specified by default.

You can configure up to eight SIP server addresses and eight SIP server domain names in an address pool. The priorities of the specified SIP servers depend on the configuration sequence. The formerly specified SIP server takes precedence over the latter one.

If you repeatedly use the **sip-server** command, the latest configuration will not overwrite the previous one.

Examples

Specify the SIP server address as 2:2::4 for the client.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] sip-server address 2:2::4
```

Specify the domain name of the SIP server as bbb.com for the client.

```
[Sysname-dhcp6-pool-1] sip-server domain-name bbb.com
```

static-bind prefix

Syntax

static-bind prefix *prefix/prefix-len* **duid** *duid* [**iaid** *iaid*] [**preferred-lifetime** *preferred-lifetime* **valid-lifetime** *valid-lifetime*]

undo static-bind prefix *prefix/prefix-len*

View

DHCPv6 address pool view

Default level

2: System level

Parameters

prefix/prefix-len: Static prefix and prefix length.

duid *duid*: Client DUID. The value is an even hexadecimal number, in the range of 2 to 256.

iaid *iaid*: Client IAID. The value is a hexadecimal number in the range of 0 to FFFFFFFF. If no IAID is specified, the server does not match against the client IAID for prefix assignment.

preferred-lifetime *preferred-lifetime*: Specifies the preferred lifetime of the prefix to be assigned. The value ranges from 60 to 4294967295, in seconds. The default value is 604800 seconds, that is, seven days.

valid-lifetime *valid-lifetime*: Specifies the valid lifetime of the prefix to be assigned. The value ranges from 60 to 4294967295, in seconds. The default value is 2592000 seconds, that is, 30 days. The valid lifetime must be greater than or equal to the preferred lifetime.

Description

Use the **static-bind prefix** command to configure a static prefix.

Use the **undo static-bind prefix** command to remove a static prefix.

No static prefix is configured by default.

After a static prefix is bound to a client, the configuration cannot be modified. You need to delete the static prefix before you can bind the prefix to another client.

Examples

Configure static prefix 2001:0410::/35 in address pool 1, and specify the DUID as 00030001CA0006A400, the IAID as A1A1A1A1, the preferred lifetime as one day, and the valid lifetime as three days.

```
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] static-bind prefix 2001:0410::/35 duid 00030001CA0006A400 iaid
A1A1A1A1 preferred-lifetime 86400 valid-lifetime 259200
```

DHCPv6 relay agent configuration commands

display ipv6 dhcp relay server-address

Syntax

display ipv6 dhcp relay server-address { **all** | **interface** *interface-type interface-number* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

all: Displays all DHCPv6 server address information.

interface *interface-type interface-number*: Displays DHCPv6 server address information of the specified interface.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display ipv6 dhcp relay server-address** command to display information about DHCPv6 server addresses specified on the DHCPv6 relay agent.

Examples

Display all the DHCPv6 server address information.

```
<Sysname> display ipv6 dhcp relay server-address all
Interface: Vlan2
Server address(es)                              Output Interface
1::1
FF02::1:2                                       Vlan4

Interface: Vlan3
Server address(es)                              Output Interface
1::1
FF02::1:2                                       Vlan4
```

Display DHCPv6 server address information of VLAN-interface 2.

```
<Sysname> display ipv6 dhcp relay server-address interface vlan-interface 2
Interface: Vlan2
Server address(es)                              Output Interface
1::1
```

```
FF02::1:2                                 Vlan4
```

Table 48 Output description

Field	Description
Interface	Interface that serves as the DHCPv6 relay agent
Server address(es)	DHCPv6 server address(es) specified on the interface
Output Interface	Outgoing interface of DHCPv6 packets

display ipv6 dhcp relay statistics

Syntax

display ipv6 dhcp relay statistics [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display ipv6 dhcp relay statistics** command to display packet statistics on the DHCPv6 relay agent.

Related commands: **reset ipv6 dhcp relay statistics**.

Examples

Display packet statistics on the DHCPv6 relay agent.

```
<Sysname> display ipv6 dhcp relay statistics
Packets dropped               :  4
    Error                     :  4
    Excess of rate limit      :  0
Packets received              :  14
    SOLICIT                   :  0
    REQUEST                   :  0
    CONFIRM                   :  0
    RENEW                     :  0
    REBIND                    :  0
    RELEASE                   :  0
    DECLINE                   :  0
    INFORMATION-REQUEST       :  7
```

```
    RELAY-FORWARD              :  0
    RELAY-REPLY                :  7
Packets sent                   :  14
    ADVERTISE                  :  0
    RECONFIGURE                :  0
    REPLY                      :  7
    RELAY-FORWARD              :  7
    RELAY-REPLY                :  0
```

Table 49 Output description

Field	Description
Packets dropped	Number of discarded packets
Error	Number of discarded error packets
Excess of rate limit	Number of packets discarded due to excess of rate limit
Packets received	Number of received packets
SOLICIT	Number of received solicit packets
REQUEST	Number of received request packets
CONFIRM	Number of received confirm packets
RENEW	Number of received renew packets
REBIND	Number of received rebind packets
RELEASE	Number of received release packets
DECLINE	Number of received decline packets
INFORMATION-REQUEST	Number of received information request packets
RELAY-FORWARD	Number of received relay-forward packets
RELAY-REPLY	Number of received relay-reply packets
Packets sent	Number of sent packets
ADVERTISE	Number of sent advertise packets
RECONFIGURE	Number of sent reconfigure packets
REPLY	Number of sent reply packets
RELAY-FORWARD	Number of sent Relay-forward packets
RELAY-REPLY	Number of sent Relay-reply packets

ipv6 dhcp relay server-address

Syntax

ipv6 dhcp relay server-address *ipv6-address* [**interface** *interface-type interface-number*]

undo ipv6 dhcp relay server-address *ipv6-address* [**interface** *interface-type interface-number*]

View

Interface view

Default level

2: System level

Parameters

ipv6-address: IPv6 address of the DHCPv6 server.

interface *interface-type interface-number*: Specifies an outgoing interface for DHCPv6 packets.

Description

Use the **ipv6 dhcp relay server-address** command to enable DHCPv6 relay agent on the interface and specify a DHCPv6 server.

Use the **undo ipv6 dhcp relay server-address** command to remove the DHCPv6 server from the interface.

By default, DHCPv6 relay agent is disabled and no DHCPv6 server is specified on the interface.

Upon receiving a request from a DHCPv6 client, the interface that operates as a DHCPv6 relay agent encapsulates the request into a Relay-forward message and forwards the message to the specified DHCPv6 server, which then assigns an IPv6 address and other configuration parameters to the DHCPv6 client.

Executing the **ipv6 dhcp relay server-address** command repeatedly can specify multiple DHCPv6 servers, and up to eight DHCP servers can be specified for an interface. After receiving requests from DHCPv6 clients, the DHCPv6 relay agent forwards the requests to all the specified DHCPv6 servers.

If the DHCPv6 server address is a link-local address or link-scoped multicast address on the local link, you need to specify an outgoing interface; otherwise, DHCPv6 packets may fail to be forwarded to the DHCPv6 server.

After you remove all the specified DHCPv6 servers from an interface with the **undo ipv6 dhcp relay server-address** command, DHCPv6 relay agent is disabled on the interface.

An interface cannot serve as a DHCPv6 client and DHCPv6 relay agent at the same time.

Related commands: **display ipv6 dhcp relay server-address**.

Examples

Enable DHCPv6 relay agent on VLAN-interface 2, and specify the DHCPv6 server address as 2001:1::3.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ipv6 dhcp relay server-address 2001:1::3
```

reset ipv6 dhcp relay statistics

Syntax

reset ipv6 dhcp relay statistics

View

User view

Default level

1: Monitor level

Parameters

None

Description

Use the **reset ipv6 dhcp relay statistics** command to clear packets statistics on the DHCPv6 relay agent.

After this command is executed, the packets statistics is displayed as 0 when you use the **display ipv6 dhcp relay statistics** command.

Related commands: **display ipv6 dhcp relay statistics**.

Examples

Clear packet statistics on the DHCPv6 relay agent.

```
<Sysname> reset ipv6 dhcp relay statistics
```

DHCPv6 client configuration commands

display ipv6 dhcp client

Syntax

display ipv6 dhcp client [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface *interface-type interface-number*: Displays the DHCPv6 client information of a specified interface.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display ipv6 dhcp client** command to display DHCPv6 client information.

With no parameters specified, the DHCPv6 client information of all the interfaces will be displayed.

Examples

Display the DHCPv6 client information of VLAN-interface 2.

```
<Sysname> display ipv6 dhcp client interface vlan-interface 2
Vlan-interface2 is in stateless DHCPv6 client mode
State is OPEN
Preferred Server:
    Reachable via address    :  FE80::213:7FFF:FEF6:C818
    DUID                     :  0003000100137ff6c818
```

```
DNS servers              :  1:2:3::5
                            1:2:4::7
Domain names             :  abc.com
```

Table 50 Output description

Field	Description
in stateless DHCPv6 client mode	Indicates the client is in the stateless DHCPv6 configuration mode.
State is OPEN	Current state of the DHCPv6 client, which can be: • INIT: After enabled, the DHCPv6 client enters the INIT state. • IDLE: After receiving an RA message with the "M" flag set to 0 and "O" flag set to 1 and enabled with stateless DHCPv6, the DHCPv6 client enters the IDLE state. • INFO-REQUESTING: The DHCPv6 client is requesting configuration information. • OPEN: The DHCPv6 client successfully obtained configuration parameters and completed stateless configuration based on the obtained parameters.
Preferred Server	Information about the DHCPv6 server selected by the DHCPv6 client
Reachable via address	Reachable address, which is the link local address of the DHCPv6 server or relay agent.
DUID	DHCP unique identifier (DUID) of the DHCPv6 server
DNS servers	DNS server address sent by the DHCPv6 server
Domain names	Domain name information sent by the DHCPv6 server

display ipv6 dhcp client statistics

Syntax

display ipv6 dhcp client statistics [**interface** *interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface *interface-type interface-number*: Displays the DHCPv6 client statistics of a specified interface.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display ipv6 dhcp client statistics** command to display DHCPv6 client statistics.

With no parameters specified, DHCPv6 client statistics of all the interfaces will be displayed.

Related commands: **reset ipv6 dhcp client statistics**.

Examples

Display DHCPv6 client statistics of VLAN-interface 2.

```
<Sysname> display ipv6 dhcp client statistics interface vlan-interface 2
Interface                    :  Vlan-interface2
Packets Received             :  1
         Reply               :  1
         Advertise           :  0
         Reconfigure         :  0
         Invalid             :  0
Packets Sent                 :  5
         Solicit             :  0
         Request             :  0
         Confirm             :  0
         Renew               :  0
         Rebind              :  0
         Information-request :  5
         Release             :  0
         Decline             :  0
```

Table 51 Output description

Field	Description
Interface	Interface that servers as the DHCPv6 client
Packets Received	Number of received packets
Reply	Number of received reply packets
Advertise	Number of received advertise packets
Reconfigure	Number of received reconfigure packets
Invalid	Number of invalid packets
Packets Sent	Number of sent packets
Solicit	Number of sent solicit packets
Request	Number of sent request packets
Confirm	Number of sent confirm packets
Renew	Number of sent renew packets
Rebind	Number of sent rebind packets
Information-request	Number of sent information request packets
Release	Number of sent release packets
Decline	Number of sent decline packets

reset ipv6 dhcp client statistics

Syntax

reset ipv6 dhcp client statistics [**interface** *interface-type interface-number*]

View

User view

Default level

1: Monitor level

Parameters

interface *interface-type interface-number*: Clears DHCPv6 client statistics of a specified interface.

Description

Use the **reset ipv6 dhcp client statistics** command to clear DHCPv6 client statistics.

With no parameters specified, DHCPv6 client statistics of all the interfaces will be cleared.

After this command is executed, the packets statistics is displayed as 0 when you use the **display ipv6 dhcp client statistics** command.

Related commands: **display ipv6 dhcp client statistics**.

Examples

Clear DHCPv6 client statistics of all the interfaces.

```
<Sysname> reset ipv6 dhcp client statistics
```

DHCPv6 snooping configuration commands

display ipv6 dhcp snooping trust

Syntax

display ipv6 dhcp snooping trust [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display ipv6 dhcp snooping trust** command to display DHCPv6 snooping trusted ports.

Examples

Display DHCPv6 snooping trusted ports.

```
<Sysname> display ipv6 dhcp snooping trust
 Trusted ports include:
GigabitEthernet1/0/1
GigabitEthernet1/0/2
```

display ipv6 dhcp snooping user-binding

Syntax

display ipv6 dhcp snooping user-binding { *ipv6-address* | **dynamic** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

ipv6-address: Displays DHCPv6 snooping entries of the specified IPv6 address.

dynamic: Displays all DHCPv6 snooping entries.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see the *Fundamentals Configuration Guide*.

begin: Displays the first line that matches the specified regular expression and all lines that follow.

exclude: Displays all lines that do not match the specified regular expression.

include: Displays all lines that match the specified regular expression.

regular-expression: Specifies a regular expression, which is a case sensitive string of 1 to 256 characters.

Description

Use the **display ipv6 dhcp snooping user-binding** command to display DHCPv6 snooping entries.

Examples

Display all DHCPv6 snooping entries.

```
<Sysname> display ipv6 dhcp snooping user-binding dynamic
IPv6 Address                    MAC Address    Lease      VLAN Interface
============================== ============== ========== ==== ==================
2::1                            00e0-fc00-0006 286        1    GigabitEthernet1/0/1
---   1 DHCPv6 snooping item(s) found   ---
```

Table 52 Output description

Field	Description
IPv6 Address	IPv6 address in the DHCPv6 snooping entry
MAC Address	MAC address in the DHCPv6 snooping entry

Field	Description
Lease	Remaining lease of the DHCPv6 snooping entry, in seconds.
VLAN	VLAN to which the interface belongs
Interface	Interface through which the DHCPv6 client is connected

ipv6 dhcp snooping enable

Syntax

ipv6 dhcp snooping enable

undo ipv6 dhcp snooping enable

View

System view

Default level

2: System level

Parameters

None

Description

Use the **ipv6 dhcp snooping enable** command to enable DHCPv6 snooping globally.

Use the **undo ipv6 dhcp snooping enable** command to disable DHCPv6 snooping globally.

By default, global DHCPv6 snooping is disabled.

After DHCPv6 snooping is enabled in system view, the DHCPv6 snooping device discards DHCPv6 reply messages received by an untrusted port if any, and does not record these DHCPv6 snooping entries.

Examples

Enable DHCPv6 snooping globally.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping enable
```

ipv6 dhcp snooping max-learning-num

Syntax

ipv6 dhcp snooping max-learning-num *number*

undo ipv6 dhcp snooping max-learning-num

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

number: Maximum number of DHCPv6 snooping entries an interface can learn. The value ranges from 0 to 1024.

Description

Use the **ipv6 dhcp snooping max-learning-num** command to configure the maximum number of DHCPv6 snooping entries an interface can learn.

Use the **undo ipv6 dhcp snooping max-learning-num** command to restore the default.

By default, the number of DHCPv6 snooping entries learned by an interface is not limited.

Examples

Set the maximum number of DHCPv6 snooping entries Layer 2 Ethernet interface GigabitEthernet 1/0/1 can learn to 1000.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping max-learning-num 1000
```

ipv6 dhcp snooping trust

Syntax

ipv6 dhcp snooping trust

undo ipv6 dhcp snooping trust

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

None

Description

Use the **ipv6 dhcp snooping trust** command to configure a DHCPv6 trusted port.

Use the **undo ipv6 dhcp snooping trust** command to restore the default.

By default, all interfaces of a switch with DHCPv6 snooping enabled globally are untrusted ports.

After DHCPv6 snooping is enabled, to ensure that DHCPv6 clients can obtain IPv6 addresses from an authorized DHCPv6 server, you need to configure the port that connects to the authorized DHCPv6 server as a trusted port.

Examples

Configure Ethernet interface GigabitEthernet 1/0/1 as a trusted port.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping trust
```

ipv6 dhcp snooping vlan enable

Syntax

ipv6 dhcp snooping vlan enable

undo ipv6 dhcp snooping vlan enable

View

VLAN view

Default level

2: System level

Parameters

None

Description

Use the **ipv6 dhcp snooping vlan enable** command to enable DHCPv6 snooping for a specific VLAN.

Use the **undo ipv6 dhcp snooping vlan enable** command to disable DHCPv6 snooping for a specific VLAN.

By default, DHCPv6 snooping is disabled for a VLAN.

After DHCPv6 snooping is enabled globally and then enabled for a VLAN, the DHCPv6 snooping device records DHCPv6 snooping entries according to the DHCPv6 packets received in the VLAN. Meanwhile, upon receiving a DHCPv6 request from a client in the VLAN, the device forwards the packet through trusted ports rather than any untrusted port in the VLAN, thus reducing network traffic.

Examples

Enable DHCPv6 snooping for VLAN 1.

```
<Sysname> system-view
[Sysname] vlan 1
[Sysname-vlan1] ipv6 dhcp snooping vlan enable
```

reset ipv6 dhcp snooping user-binding

Syntax

reset ipv6 dhcp snooping user-binding { *ipv6-address* | **dynamic** }

View

User view

Default level

2: System level

Parameters

ipv6-address: Clears DHCPv6 snooping entries of the specified IPv6 address.

dynamic: Clears all DHCPv6 snooping entries.

Description

Use the **reset ipv6 dhcp snooping user-binding** command to clear DHCPv6 snooping entries.

Examples

Clear all DHCPv6 snooping entries.

```
<Sysname> reset ipv6 dhcp snooping user-binding dynamic
```

Support and other resources

Contacting HP

For worldwide technical support information, see the HP support website:

http://www.hp.com/support

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

http://www.hp.com/go/wwalerts

After registering, you will receive email notification of product enhancements, new driver versions, firmware updates, and other product resources.

Related information

Documents

To find related documents, browse to the Manuals page of the HP Business Support Center website:

http://www.hp.com/support/manuals

- For related documentation, navigate to the Networking section, and select a networking category.
- For a complete list of acronyms and their definitions, see *HP FlexNetwork Technology Acronyms*.

Websites

- HP.com http://www.hp.com
- HP Networking http://www.hp.com/go/networking
- HP manuals http://www.hp.com/support/manuals
- HP download drivers and software http://www.hp.com/support/downloads
- HP software depot http://www.software.hp.com
- HP Education http://www.hp.com/learn

Conventions

This section describes the conventions used in this documentation set.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk-marked braces enclose a set of required syntax choices separated by vertical bars, from which you select at least one.
[x | y | ...] *	Asterisk-marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in bold text. For example, the **New User** window appears; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT	An alert that calls attention to essential information.
NOTE	An alert that contains additional or supplementary information.
TIP	An alert that provides helpful information.

Network topology icons

	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the switching engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a security product, such as a firewall, a UTM, or a load-balancing or security card that is installed in a device.
	Represents a security card, such as a firewall card, a load-balancing card, or a NetStream card.

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

Index

E

F

G

I

N

O

P

R

S

T

U

V