

HP 5500 EI & 5500 SI Switch Series

Layer 3 - IP Services

Command Reference

Part number: 5998-1719

Software version: Release 2220

Document version: 6W100-20130810



Legal and notice information

© Copyright 2013 Hewlett-Packard Development Company, L.P.

No part of this documentation may be reproduced or transmitted in any form or by any means without prior written consent of Hewlett-Packard Development Company, L.P.

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	1
arp check enable	1
arp max-learning-num	1
arp static	2
arp timer aging	3
display arp	4
display arp <i>ip-address</i>	5
display arp timer aging	6
display arp vpn-instance (available only on the HP 5500 EI)	7
mac-address station-move	7
reset arp	8
Gratuitous ARP configuration commands	9
arp send-gratuitous-arp	9
arp ip-conflict prompt	10
gratuitous-arp-sending enable	10
gratuitous-arp-learning enable	11
Proxy ARP configuration commands	12
display local-proxy-arp	12
display proxy-arp	12
local-proxy-arp enable	13
proxy-arp enable	14
ARP snooping configuration commands	15
arp-snooping enable	15
display arp-snooping	15
reset arp-snooping	16
IP addressing configuration commands	17
display ip interface	17
display ip interface brief	19
ip address	21
ip address unnumbered (available only on the HP 5500 EI)	22
DHCP server configuration commands	23
bims-server	23
bootfile-name	23
dhcp dscp (for DHCP server)	24
dhcp enable (for DHCP server)	25
dhcp server apply ip-pool	25
dhcp select server global-pool	26
dhcp server client-detect enable	27
dhcp server detect	27
dhcp server forbidden-ip	28
dhcp server ip-pool	29
dhcp server ping packets	29
dhcp server ping timeout	30
dhcp server relay information enable	31
dhcp server threshold	31
display dhcp server conflict	32

display dhcp server expired	33
display dhcp server free-ip	34
display dhcp server forbidden-ip	35
display dhcp server ip-in-use	36
display dhcp server statistics	37
display dhcp server tree	39
dns-list	40
domain-name	41
expired	42
forbidden-ip	42
gateway-list	43
nbns-list	44
netbios-type	45
network	45
network ip range	46
network mask	47
next-server	48
option	48
reset dhcp server conflict	49
reset dhcp server ip-in-use	49
reset dhcp server statistics	50
static-bind client-identifier	50
static-bind ip-address	51
static-bind mac-address	52
tftp-server domain-name	53
tftp-server ip-address	53
vendor-class-identifier	54
voice-config	55

DHCP relay agent configuration commands	57
dhcp dscp (for DHCP relay agent)	57
dhcp enable (for DHCP relay agent)	57
dhcp relay address-check enable	58
dhcp relay check mac-address	59
dhcp relay client-detect enable	59
dhcp relay information circuit-id format-type	60
dhcp relay information circuit-id string	61
dhcp relay information enable	61
dhcp relay information format	62
dhcp relay information remote-id format-type	63
dhcp relay information remote-id string	63
dhcp relay information strategy	64
dhcp relay release ip	65
dhcp relay security static	65
dhcp relay security refresh enable	66
dhcp relay security tracker	67
dhcp relay server-detect	67
dhcp relay server-group	68
dhcp relay server-select	69
dhcp select relay	70
display dhcp relay	70
display dhcp relay information	71
display dhcp relay security	73
display dhcp relay security statistics	74
display dhcp relay security tracker	74

display dhcp relay server-group	75
display dhcp relay statistics	76
reset dhcp relay statistics	78
DHCP client configuration commands	79
display dhcp client	79
dhcp client dscp	81
ip address dhcp-alloc	81
DHCP snooping configuration commands	83
dhcp-snooping	83
dhcp-snooping binding database filename	83
dhcp-snooping binding database update interval	84
dhcp-snooping binding database update now	85
dhcp-snooping check mac-address	85
dhcp-snooping check request-message	86
dhcp-snooping information circuit-id format-type	86
dhcp-snooping information circuit-id string	87
dhcp-snooping information enable	88
dhcp-snooping information format	89
dhcp-snooping information remote-id format-type	90
dhcp-snooping information remote-id string	90
dhcp-snooping information strategy	91
dhcp-snooping information sub-option	92
dhcp-snooping rate-limit	93
dhcp-snooping trust	94
display dhcp-snooping	94
display dhcp-snooping binding database	95
display dhcp-snooping information	96
display dhcp-snooping packet statistics	98
display dhcp-snooping trust	98
reset dhcp-snooping	99
reset dhcp-snooping packet statistics	100
BOOTP client configuration commands	101
display bootp client	101
ip address bootp-alloc	102
IPv4 DNS configuration commands	103
display dns domain	103
display dns host	104
display dns server	105
display ip host	106
dns domain	107
dns dscp	107
dns proxy enable	108
dns resolve	108
dns server	109
dns source-interface	110
dns spoofing	110
ip host	111
reset dns host	112
IRDP configuration commands	113
ip irdp	113
ip irdp address	113
ip irdp lifetime	114

ip irdp maxadvinterval	114
ip irdp minadvinterval	115
ip irdp multicast	116
ip irdp preference	116
IP performance optimization configuration commands	118
display fib	118
display fib <i>ip-address</i>	120
display icmp statistics	121
display ip socket	122
display ip statistics	125
display tcp statistics	127
display udp statistics	129
ip forward-broadcast (interface view)	130
ip forward-broadcast (system view)	131
ip redirects enable	132
ip ttl-expires enable	132
ip unreachable enable	133
reset ip statistics	133
reset tcp statistics	134
reset udp statistics	134
tcp path-mtu-discovery	134
tcp timer fin-timeout	135
tcp timer syn-timeout	136
tcp window	136
UDP helper configuration commands	138
display udp-helper server	138
reset udp-helper packet	138
udp-helper enable	139
udp-helper port	139
udp-helper server	140
IPv6 basics configuration commands	142
display ipv6 fib	142
display ipv6 fib <i>ipv6-address</i>	143
display ipv6 interface	145
display ipv6 nd snooping	149
display ipv6 neighbors	150
display ipv6 neighbors count	152
display ipv6 neighbors vpn-instance (available only on the HP 5500 EI)	153
display ipv6 pathmtu	154
display ipv6 socket	155
display ipv6 statistics	157
display tcp ipv6 statistics	161
display tcp ipv6 status	163
display udp ipv6 statistics	164
ipv6	165
ipv6 address	166
ipv6 address anycast	166
ipv6 address auto	167
ipv6 address auto link-local	168
ipv6 address eui-64	168
ipv6 address link-local	169
ipv6 hoplimit-expires enable	170
ipv6 icmp-error	170

ipv6 icmpv6 multicast-echo-reply enable	171
ipv6 nd autoconfig managed-address-flag	171
ipv6 nd autoconfig other-flag	172
ipv6 nd dad attempts	173
ipv6 nd hop-limit	173
ipv6 nd ns retrans-timer	174
ipv6 nd nud reachable-time	174
ipv6 nd ra halt	175
ipv6 nd ra interval	176
ipv6 nd ra no-advlinkmtu	176
ipv6 nd ra prefix	177
ipv6 nd ra router-lifetime	178
ipv6 nd snooping enable	178
ipv6 nd snooping enable global	179
ipv6 nd snooping enable link-local	179
ipv6 nd snooping max-learning-num	180
ipv6 nd snooping uplink	181
ipv6 neighbor	181
ipv6 neighbor stale-aging	182
ipv6 neighbors max-learning-num	183
ipv6 pathmtu	183
ipv6 pathmtu age	184
ipv6 prefer temporary-address	185
ipv6 unreachable enable	185
local-proxy-nd enable	186
proxy-nd enable	186
reset ipv6 nd snooping	187
reset ipv6 neighbors	187
reset ipv6 pathmtu	188
reset ipv6 statistics	189
reset tcp ipv6 statistics	189
reset udp ipv6 statistics	190
tcp ipv6 timer fin-timeout	190
tcp ipv6 timer syn-timeout	191
tcp ipv6 window	191

DHCPv6 configuration commands 192

DHCPv6 common configuration commands	192
display ipv6 dhcp duid	192
DHCPv6 server configuration commands	192
display ipv6 dhcp pool	192
display ipv6 dhcp prefix-pool	194
display ipv6 dhcp server	195
display ipv6 dhcp server pd-in-use	196
display ipv6 dhcp server statistics	198
dns-server	200
domain-name	200
ds-lite address	201
ipv6 dhcp dscp (for DHCPv6 server)	201
ipv6 dhcp pool	202
ipv6 dhcp prefix-pool	203
ipv6 dhcp server apply pool	203
ipv6 dhcp server enable	204
prefix-pool	205
reset ipv6 dhcp server pd-in-use	206

reset ipv6 dhcp server statistics	206
sip-server	207
static-bind prefix	208
DHCPv6 relay agent configuration commands	209
display ipv6 dhcp relay server-address	209
display ipv6 dhcp relay statistics	210
ipv6 dhcp dscp (for DHCPv6 relay agent)	211
ipv6 dhcp relay server-address	212
reset ipv6 dhcp relay statistics	213
DHCPv6 client configuration commands	213
display ipv6 dhcp client	213
display ipv6 dhcp client statistics	215
ipv6 dhcp client dscp	216
reset ipv6 dhcp client statistics	217
DHCPv6 snooping configuration commands	217
display ipv6 dhcp snooping trust	217
display ipv6 dhcp snooping user-binding	218
ipv6 dhcp snooping enable	219
ipv6 dhcp snooping max-learning-num	219
ipv6 dhcp snooping option interface-id enable	220
ipv6 dhcp snooping option interface-id string	221
ipv6 dhcp snooping option remote-id enable	221
ipv6 dhcp snooping option remote-id string	222
ipv6 dhcp snooping trust	222
ipv6 dhcp snooping vlan enable	223
reset ipv6 dhcp snooping user-binding	224
IPv6 DNS configuration commands	225
display dns ipv6 server	225
display ipv6 host	226
dns ipv6 dscp	227
dns server ipv6	227
ipv6 host	228
Tunneling configuration commands (available only on the HP 5500 EI)	229
default	229
description	229
destination	230
display interface tunnel	231
display ipv6 interface tunnel	234
interface tunnel	238
mtu	238
reset counters interface	239
service-loopback-group	239
shutdown	240
source	241
tunnel bandwidth	242
tunnel discard ipv4-compatible-packet	242
tunnel-protocol	243
Support and other resources	245
Contacting HP	245
Subscription service	245
Related information	245
Documents	245
Websites	245

Conventions	246
Index	248

ARP configuration commands

Only the HP 5500 EI switches support Layer 3 Ethernet port configuration.

You can use the **port link-mode** command to set an Ethernet port to operate in bridge (Layer 2) or route mode (Layer 3) (see *Layer 2—LAN Switching Configuration Guide*).

arp check enable

Syntax

```
arp check enable
undo arp check enable
```

View

System view

Default level

2: System level

Parameters

None

Description

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

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

By default, dynamic ARP entry check is enabled.

Examples

```
# Enable dynamic 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

Layer 2 Ethernet interface view, Layer 3 Ethernet interface view, VLAN interface view, Layer 2 aggregate interface view, Layer 3 aggregate interface view

Default level

2: System level

Parameters

number: Specifies the maximum number of dynamic ARP entries that an interface can learn.

- On the HP 5500 EI switch series, the *number* argument ranges from 0 to 8192.
- On the HP 5500 SI switch series, the *number* argument ranges from 0 to 2048.

Description

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

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

By default, a Layer 2 interface does not limit the number of dynamic ARP entries. A Layer 3 interface on the HP 5500 EI switch series can learn up to 8192 dynamic ARP entries. A Layer 3 interface on the HP 5500 SI switch series can learn up to 2048 dynamic ARP entries.

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
```

Specify Layer 3 aggregate interface route-aggregation 1 to learn up to 100 dynamic ARP entries.

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

arp static

Syntax

```
arp static ip-address mac-address [ vlan-id interface-type interface-number ] [ vpn-instance vpn-instance-name ]
```

```
undo arp ip-address [ vpn-instance-name ]
```

View

System view

Default level

2: System level

Parameters

ip-address: Specifies the IP address in an ARP entry.

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

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

interface-type interface-number: Specifies the interface type and interface number.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN for a static ARP entry. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Without this option, the static ARP entry belongs to the public network. This keyword and argument combination is available only on the HP 5500 EI series switches.

Description

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

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

A static ARP entry is effective when the device 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 be in 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 IP address 202.38.10.2, MAC address 00e0-fc01-0000, and
outbound interface 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: Specifies the age timer for dynamic ARP entries in minutes, ranging from 1 to 1440.

Description

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

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

By default, the age timer for dynamic ARP entries is 20 minutes.

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

Examples

```
# Set the age timer 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 | verbose ] [ | { 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 on a specific IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

vlan *vlan-id*: Displays the ARP entries of the specified VLAN. The VLAN ID ranges from 1 to 4094.

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.

verbose: Displays detailed information about ARP entries. This keyword is available only on the HP 5500 EI series switches.

|: 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, a case-sensitive string of 1 to 256 characters.

Description

Use **display arp** 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 information of all ARP entries.
```

```
<Sysname> display arp all
```

		Type: S-Static	D-Dynamic			
IP Address	MAC Address	VLAN ID	Interface	Aging Type		
192.168.0.235	00e0-fc02-2181	1	GE1/0/30	20	D	
192.168.0.86	00e0-fc00-7801	1	GE1/0/30	9	D	
192.168.0.161	000f-e000-0003	1	GE1/0/30	20	D	
192.168.0.162	00e0-fc14-000b	1	GE1/0/30	20	D	

Table 1 Command output

Field	Description
IP Address	IP address in an ARP entry.
MAC Address	MAC address in an ARP entry.
VLAN ID	ID of the VLAN to which the ARP entry belongs.
Interface	Outbound interface in an ARP entry.
Aging	Aging time for a dynamic ARP entry in minutes. (N/A means unknown aging time or no aging time. To display the aging time of such an entry, display ARP entries on the specified device.)
Type	ARP entry type: <ul style="list-style-type: none">• D—Dynamic.• S—Static.

Display the number of all ARP entries.

```
<Sysname> display arp all count
Total Entry(ies): 4
```

display arp ip-address

Syntax

```
display arp ip-address [ slot slot-number ] [ verbose ] [ | { 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 on a specific IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

verbose: Displays the detailed information about ARP entries. This keyword is available only on the HP 5500 EI series switches.

|: 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, a case-sensitive string of 1 to 256 characters.

Description

Use **display arp** *ip-address* to display the ARP entry for a specific 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, a case-sensitive string of 1 to 256 characters.

Description

Use **display arp timer aging** 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)
```

display arp vpn-instance (available only on the HP 5500 EI)

Syntax

```
display arp vpn-instance vpn-instance-name [ count ] [ | { begin | exclude | include }  
regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance-name: Specifies the name of an MPLS L3VPN, a case-sensitive string of 1 to 31 characters.

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, a case-sensitive string of 1 to 256 characters.

Description

Use **display arp vpn-instance** to display the ARP entries for a specific VPN.

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

Examples

Display ARP entries for the VPN instance named **test**.

```
<Sysname> display arp vpn-instance test  
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
```

mac-address station-move

Syntax

```
mac-address station-move quick-notify enable
```

```
undo mac-address station-move quick-notify enable
```

View

System view

Default level

2: System level

Parameters

None

Description

Use **mac-address station-move quick-notify enable** to enable ARP quick update.

Use **undo mac-address station-move quick-notify enable** to restore the default.

By default, ARP quick update is disabled.

Example

```
# Enable ARP quick update.
<Sysname> system-view
[Sysname] mac-address station-move quick-notify enable
```

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 on a specific IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

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

Description

Use **reset arp** 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

Layer 3 Ethernet interface view, Layer 3 aggregate interface 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 of 200 to 200000 milliseconds. The default value is 2000.

Description

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

Use **undo arp send-gratuitous-arp** 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.

The IP address contained in a gratuitous ARP request can be the VRRP virtual IP address, the primary IP address or a manually configured secondary IP address of the sending interface only. The primary IP address can be configured manually or automatically, whereas the secondary IP address must be configured manually.

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 **gratuitous-arp-sending enable** to enable a device to send gratuitous ARP packets when receiving ARP requests from another network segment.

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

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

Examples

```
# Disable a device 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 **gratuitous-arp-learning enable** to enable the gratuitous ARP packet learning function.

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

By default, the function is enabled.

With this function enabled, a device receiving a gratuitous ARP packet can add the source IP and MAC addresses to its own dynamic ARP table if it finds that no ARP entry exists in the cache corresponding to the source IP address of the ARP packet. If a matching ARP entry is found in the cache, the device 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
```

Proxy ARP configuration commands

display local-proxy-arp

Syntax

```
display local-proxy-arp [ 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 the local proxy ARP status of the interface specified by the argument *interface-type 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, a case-sensitive string of 1 to 256 characters.

Description

Use **display local-proxy-arp** to display the status of the local proxy ARP.

If no interface is specified, the local proxy ARP status of all interfaces is displayed.

Related commands: **local-proxy-arp enable**.

Examples

```
# Display the status of the local proxy ARP on VLAN-interface 2.
<Sysname> display local-proxy-arp interface vlan-interface 2
Interface Vlan-interface2
  Local Proxy ARP status: enabled
```

display proxy-arp

Syntax

```
display proxy-arp [ 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 the proxy ARP status of the interface specified by the argument *interface-type 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, a case-sensitive string of 1 to 256 characters.

Description

Use **display proxy-arp** to display the proxy ARP status.

If an interface is specified, the proxy ARP status of the specified interface is displayed; if no interface is specified, the proxy ARP status of all interfaces is displayed.

Related commands: **proxy-arp enable**.

Examples

```
# Display the proxy ARP status on VLAN-interface 1.
<Sysname> display proxy-arp interface Vlan-interface 1
Interface Vlan-interface 1
Proxy ARP status: disabled
```

local-proxy-arp enable

Syntax

local-proxy-arp enable [**ip-range** *startIP to endIP*]

undo local-proxy-arp enable

View

VLAN interface view, Layer 3 Ethernet interface view, Layer 3 aggregate interface view

Default level

2: System level

Parameters

ip-range *startIP to endIP*: Specifies the IP address range for which local proxy ARP is enabled. The start IP address must be lower than or equal to the end IP address.

Description

Use **local-proxy-arp enable** to enable local proxy ARP.

Use **undo local-proxy-arp enable** to disable local proxy ARP.

By default, local proxy ARP is disabled.

Only one IP address range can be specified by using the **ip-range** keyword on an interface.

Related commands: **display local-proxy-arp**.

Examples

```
# Enable local proxy ARP on VLAN-interface 2.
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] local-proxy-arp enable

# Enable local proxy ARP on VLAN-interface 2 for a specific IP address range.
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] local-proxy-arp enable ip-range 1.1.1.1 to 1.1.1.20
```

proxy-arp enable

Syntax

```
proxy-arp enable
undo proxy-arp enable
```

View

VLAN interface view, Layer 3 Ethernet interface view, Layer 3 aggregate interface view

Default level

2: System level

Parameters

None

Description

Use **proxy-arp enable** to enable proxy ARP.

Use **undo proxy-arp enable** to disable proxy ARP.

By default, proxy ARP is disabled.

Related commands: **display proxy-arp**.

Examples

```
# Enable proxy ARP on VLAN-interface 2.
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] proxy-arp 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 **arp-snooping enable** to enable ARP snooping.

Use **undo arp-snooping enable** 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 information for the 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, a case-sensitive string of 1 to 256 characters.

Description

Use **display arp-snooping** to display ARP snooping entries. If no keywords or arguments are specified, the command displays all the 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 entry of a specific IP address.

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

Description

Use **reset arp-snooping** 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, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip interface** to display IP configuration information about a specific Layer 3 interface or all Layer 3 interfaces.

Examples

```
# Display IP configuration information about interface VLAN-interface 1.
```

```
<Sysname> display ip interface vlan-interface 1
Vlan-interfacel 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 Command output

Field	Description
current state	<p>Current physical state of the interface:</p> <ul style="list-style-type: none"> • Administrative DOWN—The interface is shut down with the shutdown command. • DOWN—The interface is administratively up but its physical state is down, which may be caused by a connection or link failure. • UP—Both the administrative and physical states of the interface are up.
Line protocol current state	<p>Current state of the link layer protocol, which can be:</p> <ul style="list-style-type: none"> • DOWN—The protocol state of the interface is down. • UP—The protocol state of the interface is up. • UP (spoofing)—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	<p>IP address of an interface:</p> <ul style="list-style-type: none"> • Primary—Identifies a primary IP address. • Sub—Identifies a secondary IP address. • unnumbered—Identifies an unnumbered IP address. • acquired via DHCP—Identifies an IP address obtained through DHCP. • acquired via BOOTP—Identifies an IP address obtained through BOOTP. • Cluster—Identifies a cluster IP address. • Mad—Identifies a MAD IP address.
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 device startup).

Field	Description
ARP packet input number:	Total number of ARP packets received on the interface (the statistics start at the device startup), including:
Request packet:	<ul style="list-style-type: none"> • ARP request packets.
Reply packet:	<ul style="list-style-type: none"> • ARP reply packets.
Unknown packet:	<ul style="list-style-type: none"> • Unknown packets.
TTL invalid packet number	Number of TTL-invalid packets received on the interface (the statistics start at the device startup).
ICMP packet input number:	Total number of ICMP packets received on the interface (the statistics start at the device startup), including:
Echo reply:	<ul style="list-style-type: none"> • Echo reply packets.
Unreachable:	<ul style="list-style-type: none"> • Unreachable packets.
Source quench:	<ul style="list-style-type: none"> • Source quench packets.
Routing redirect:	<ul style="list-style-type: none"> • Routing redirect packets.
Echo request:	<ul style="list-style-type: none"> • Echo request packets.
Router advert:	<ul style="list-style-type: none"> • Router advertisement packets.
Router solicit:	<ul style="list-style-type: none"> • Router solicitation packets.
Time exceed:	<ul style="list-style-type: none"> • Time exceeded packets.
IP header bad:	<ul style="list-style-type: none"> • IP header bad packets.
Timestamp request:	<ul style="list-style-type: none"> • Timestamp request packets.
Timestamp reply:	<ul style="list-style-type: none"> • Timestamp reply packets.
Information request:	<ul style="list-style-type: none"> • Information request packets.
Information reply:	<ul style="list-style-type: none"> • Information reply packets.
Netmask request:	<ul style="list-style-type: none"> • Netmask request packets.
Netmask reply:	<ul style="list-style-type: none"> • Netmask reply packets.
Unknown type:	<ul style="list-style-type: none"> • 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: Specifies an interface by its type.

interface-number: Specifies an interface by its 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, a case-sensitive string of 1 to 256 characters.

Description

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

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

Related commands: **display ip interface**.

Examples

Display brief IP configuration information about VLAN interfaces.

```
<Sysname> display ip interface vlan-interface brief
```

```
*down: administratively down
```

```
(s): spoofing
```

Interface	Physical	Protocol	IP Address	Description
Vlan1	up	up	6.6.6.6	Vlan-inte...
Vlan2	up	up	7.7.7.7	Vlan-inte...

Table 3 Command output

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 may have no link present even when its link layer protocol is displayed up or the link is set up only on demand.
Interface	Interface name.
Physical	Physical state of the interface: <ul style="list-style-type: none">• *down—The interface is administratively down; that is, the interface is shut down with the shutdown command.• down—The interface is administratively up but its physical state is down.• up—Both the administrative and physical states of the interface are up.
Protocol	Link layer protocol state of the interface: <ul style="list-style-type: none">• down—The protocol state of the interface is down.• up—That the protocol state of the interface is up.• up(s)—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 up to 12 characters can be displayed. If there are more than 12 characters, only the first nine characters are displayed.

ip address

Syntax

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

View

Interface view

Default level

2: System level

Parameters

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

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

mask: Specifies the subnet mask in dotted decimal notation.

sub: Specifies the secondary IP address for the interface.

Description

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

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

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

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

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

When assigning IP addresses to an interface, consider the following:

- You can assign only one primary IP address to an interface.
- The primary and secondary IP addresses can be located in the same network segment.
- Before removing the primary IP address, remove all secondary IP addresses.
- You cannot assign a secondary IP address to the interface that is configured to obtain one through BOOTP or DHCP.

Related commands: **display ip interface**.

Examples

```
# Assign VLAN-interface 1 a primary IP address 129.12.0.1 and a secondary IP address 202.38.160.1,  
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
```

```
[Sysname-Vlan-interface1] ip address 202.38.160.1 255.255.255.0 sub
```

ip address unnumbered (available only on the HP 5500 EI)

Syntax

```
ip address unnumbered interface interface-type interface-number  
undo ip address unnumbered
```

View

Interface view

Default level

2: System level

Parameters

interface *interface-type interface-number*: Specifies an interface from which the current interface can borrow an IP address.

Description

Use **ip address unnumbered** to configure the current interface as IP unnumbered to borrow an IP address from another interface.

Use **undo ip address unnumbered** to disable IP unnumbered on the interface.

By default, the interface does not borrow IP addresses from other interfaces.

Examples

```
# Configure the interface tunnel 1 to borrow the IP address of the interface VLAN-interface 100.  
<Sysname> system-view  
[Sysname] interface Tunnel 1  
[Sysname-Tunnel1] ip address unnumbered interface vlan-interface 100
```

DHCP server configuration commands

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

Use **undo bims-server** 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 overwrites 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, and 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: Specifies the boot file name, a string of 1 to 63 characters.

Description

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

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

By default, no bootfile name is specified.

If you execute the **bootfile-name** command repeatedly, the latest configuration overwrites 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 dscp (for DHCP server)

Syntax

```
dhcp dscp dscp-value  
undo dhcp dscp
```

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value in DHCP packets, in the range of 0 to 63.

Description

Use **dhcp dscp** to set the DSCP value for DHCP packets sent by the DHCP server.

Use **undo dhcp dscp** to restore the default.

By default, the DSCP value in DHCP packets sent by the DHCP server is 56.

Examples

```
# Set the DSCP value to 30 for DHCP packets.  
<Sysname> system-view  
[Sysname] dhcp dscp 30
```

dhcp enable (for DHCP server)

Syntax

```
dhcp enable
undo dhcp enable
```

View

System view

Default level

2: System level

Parameters

None

Description

Use **dhcp enable** to enable DHCP.

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

By default, DHCP is disabled.

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

Use **undo dhcp server apply ip-pool** 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 **dhcp select server global-pool** to enable the DHCP server on specified interfaces. After the interface receives a DHCP request from a client, the DHCP server will allocate an IP address from the address pool.

Use **undo dhcp select server global-pool** 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 client-detect enable

Syntax

```
dhcp server client-detect enable
undo dhcp server client-detect enable
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **dhcp server client-detect enable** to enable client off-line detection on the DHCP server.

Use **undo dhcp server client-detect enable** to disable the function.

By default, the function is disabled.

With this feature enabled, the DHCP server considers a DHCP client goes offline when the ARP entry for the client ages out. In addition, it removes the client's IP-to-MAC binding entry.

Examples

```
# Enable client off-line detection on the DHCP server.
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp server client-detect enable
```

dhcp server detect

Syntax

```
dhcp server detect
undo dhcp server detect
```

View

System view

Default level

2: System level

Parameters

None

Description

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

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

By default, the function is disabled.

With this function enabled, upon receiving a DHCP request, the DHCP server resolves 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 use this information to check for 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: Specifies the start IP address of the IP address range to be excluded from dynamic allocation.

high-ip-address: Specifies the 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 **dhcp server forbidden-ip** to exclude IP addresses from dynamic allocation.

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

Use **undo dhcp server ip-pool** 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: Specifies the number of ping packets, in the range of 0 to 10. 0 means no ping operation.

Description

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

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

The number defaults to 1.

To avoid IP address conflicts, the DHCP server checks whether an IP address is in use before assigning it to a DHCP client.

The DHCP server pings the IP address to be assigned by using ICMP. If the server gets a response within the specified period, the server selects and pings another IP address. If not, the server pings the IP address again until the specified number of ping attempts is reached. If still no response is received, the server assigns the IP address to the requesting client.

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

Description

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

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

The time defaults to 500 ms.

To avoid IP address conflicts, the DHCP server checks whether an IP address is in use before assigning it to a DHCP client.

The DHCP server pings the IP address to be assigned by using ICMP. If the server gets a response within the specified interval, the server selects and pings another IP address. If not, the server pings the IP address again until the specified number of ping attempts is reached. If still no response is received, the server assigns the IP address to the requesting client.

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

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

Use **undo dhcp server threshold** 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 specific IP address.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp server conflict** 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 Command output

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 lease expiration information about all DHCP address pools.

ip *ip-address*: Displays lease expiration information about a specific IP address.

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

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp server expired** to display lease expiration information about specified DHCP address pools 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 Command output

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 *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp server free-ip** 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 10.0.0.1           to 10.0.0.254
```

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 *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp server forbidden-ip** 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 Command output

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 binding information about all DHCP address pools.

ip ip-address: Displays binding information about a specific IP address.

pool [pool-name]: Displays binding information about a specific address pool. The *pool name* is a string of 1 to 35 characters. If no *pool name* is specified, this command displays binding information about all address pools.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp server ip-in-use** to display binding information about DHCP address pools or an IP address.

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

Examples

```
# Display binding information about all DHCP address pools.
```

```
<Sysname> display dhcp server ip-in-use all
```

```
Pool utilization: 0.39%
```

IP address	Client-identifier/ Hardware address	Lease expiration	Type
10.1.1.1	4444-4444-4444	NOT Used	Manual
10.1.1.2	3030-3030-2e30-3030- 662e-3030-3033-2d45- 7468-6572-6e65-7430- 2f31	May 1 2009 14:02:49	Auto:COMMITTED

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

Table 7 Command output

Field	Description
Pool utilization	<p>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.</p> <ul style="list-style-type: none"> When binding information about all DHCP address pools is displayed, this field displays the total utilization rate of IP addresses in all DHCP address pools. When binding information about a specific DHCP address pool is displayed, this field displays the utilization rate of IP addresses in the DHCP address pool. When binding information about 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.
Lease expiration	<p>Lease expiration time:</p> <ul style="list-style-type: none"> 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	<p>Binding types:</p> <ul style="list-style-type: none"> 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.

In the output from the **display dhcp server ip-in-use** command, the lease duration of a used static binding is displayed as Unlimited instead of the actual lease duration. To display the actual lease duration, use the **display this** command in DHCP address pool view.

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 *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp server statistics** 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
    BOOTPREREQUEST:            0
  BOOTP Reply:                6
    DHCPOFFER:                 3
    DHCPACK:                   3
    DHCPNAK:                   0
    BOOTPREPLY:                0
  Bad Messages:               0
```

Table 8 Command output

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. The requests include: <ul style="list-style-type: none">• DHCPDISCOVER.• DHCPREQUEST.• DHCPDECLINE.• DHCPRELEASE.• DHCPINFORM.• BOOTPREREQUEST.

Field	Description
BOOTP Reply	The number of DHCP replies sent from the DHCP server to DHCP clients. The replies include: <ul style="list-style-type: none"> • DHCP OFFER. • 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 about all DHCP address pools.

pool [*pool-name*]: Displays information about a specific address pool. The *pool name* argument is a string of 1 to 35 characters. If no *pool name* is specified, this command displays information about all address pools.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp server tree** to display information about DHCP address pools.

Examples

```
# Display information about 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 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 0

```

Table 9 Command output

Field	Description
Global pool	Information about a common address pool.
Pool name	Address pool name.
network	Subnet for address allocation.
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	<p>The sibling node of the current node. Nodes of this kind in the output can be:</p> <ul style="list-style-type: none"> • 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, minute, and second.
Extended pool	Information about 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>: Specifies the 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 **dns-list** to specify DNS server addresses in a DHCP address pool.

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

By default, no DNS server address is specified.

If you perform the **dns-list** command repeatedly, the latest configuration overwrites 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 **domain-name** to specify a domain name suffix for the DHCP clients in the DHCP address pool.

Use **undo domain-name** 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 [ second second ] ] ] | 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.

second *second*: Specifies the number of seconds, in the range of 0 to 59.

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

Description

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

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

By default, the lease duration of a static address pool is unlimited, and the lease duration of a dynamic address pool is one day.

The lease duration cannot be less than 5 seconds.

The lease duration can be specified and takes effect for a static binding, but the lease duration from the **display dhcp server ip-in-use all** command output is still Unlimited.

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

Examples

Specify the lease duration as one day, two hours, three minutes, and four seconds 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 second 4
```

forbidden-ip

Syntax

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

View

DHCP extended address pool view

Default level

2: System level

Parameters

ip-address&<1-8>: Specifies the 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 **forbidden-ip** to exclude IP addresses from dynamic allocation in an extended address pool.

Use **undo forbidden-ip** 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.

- 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>: Specifies the 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 **gateway-list** to specify gateway addresses in a DHCP address pool.

Use **undo gateway-list** to remove specified gateway addresses 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 overwrites 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>: Specifies the 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 **nbns-list** to specify WINS server addresses in a DHCP address pool.

Use **undo nbns-list** to remove the specified WINS server addresses.

By default, no WINS server address is specified.

If you use the **nbns-list** command repeatedly, the latest configuration overwrites 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: Specifies the broadcast node. A b-node client sends the destination name in a broadcast message to get the name-to-IP mapping from a server.

h-node: Specifies the hybrid node. An h-node client unicasts the destination name to a WINS server, and if receiving no response, then broadcasts it to get the mapping from a server.

m-node: Specifies the mixed node. An m-node client broadcasts the destination name, and if receiving no response, then unicasts the destination name to the WINS server to get the mapping.

p-node: Specifies the peer-to-peer node. A p-node client sends the destination name in a unicast message to get the mapping from the WINS server.

Description

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

Use **undo netbios-type** 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: Specifies the subnet for dynamic allocation. If no mask length and mask is specified, the natural mask will be used.

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

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

Description

Use **network** to specify the subnet for dynamic allocation in a DHCP address pool.

Use **undo network** to remove the specified subnet.

No subnet is specified by default.

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

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

Examples

```
# Specify 192.168.8.0/24 as the subnet 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: Specifies the lowest IP address for dynamic allocation.

max-address: Specifies the highest IP address for dynamic allocation.

Description

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

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

No IP address range is specified by default.

In a common address pool, you can use the **network ip range** command to further specify an IP address range on a subnet for address allocation. The specified IP address range must belong to the subnet. Otherwise, the common address pool cannot assign IP addresses.

You can specify only one IP address range for each address pool. If you use the **network ip range** command repeatedly, the latest configuration overwrites the previous one.

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

Examples

```
# Specify addresses 10.1.1.1 through 10.1.1.150 on subnet 10.1.1.0/24 for dynamic address allocation in common address pool 1.
```

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 1
[Sysname-dhcp-pool-1] network 10.1.1.0 24
[Sysname-dhcp-pool-1] network ip range 10.1.1.1 10.1.1.150
```

```
# Specify addresses 192.168.8.1 through 192.168.8.150 for dynamic address 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 extended address pool view

Default level

2: System level

Parameters

mask: Specifies a network mask, in dotted decimal notation.

Description

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

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

No IP address mask is specified by default.

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**, **display dhcp server tree**, and **network ip range**.

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
```


next-server

Syntax

next-server *ip-address*

undo next-server

View

DHCP address pool view

Default level

2: System level

Parameters

ip-address: Specifies the IP address of a server.

Description

Use **next-server** to specify the IP address of a server for DHCP clients.

Use **undo next-server** to remove the server's IP address from the DHCP address pool.

By default, no server's IP address is specified in the address pool on the DHCP server.

If you repeatedly execute this command, the new configuration overwrites the previous one.

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

Examples

```
# Specify a server's IP address 1.1.1.1 in DHCP address pool 0.
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] next-server 1.1.1.1
```

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

Use **undo option** 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 overwrites 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 specific IP address.

Description

Use **reset dhcp server conflict** to clear statistics of IP address conflicts.

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 IP address dynamic binding information about all DHCP address pools.

ip *ip-address*: Clears dynamic binding information about a specific IP address.

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

Description

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

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

Examples

```
# Clear binding information about 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

1: Monitor level

Parameters

None

Description

Use **reset dhcp server statistics** 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: 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 **static-bind client-identifier** to specify the client ID of a static binding in a DHCP address pool.

Use **undo static-bind client-identifier** 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 overwrites 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: Specifies the IP address of a static binding. If no mask and mask length is specified, the natural mask is used.

mask-length: Specifies the mask length of the IP address, which is the number of 1s in the mask, in the range of 1 to 30.

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

Description

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

Use **undo static-bind ip-address** 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 overwrites 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: Specifies the MAC address of a static binding, in the format of H-H-H.

Description

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

Use **undo static-bind mac-address** 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 overwrites 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: Specifies the TFTP server name, a string of 1 to 63 characters.

Description

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

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

By default, no TFTP server name is specified.

If you perform the **tftp-server domain-name** command repeatedly, the last configuration overwrites the previous one.

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: Specifies the TFTP server IP address.

Description

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

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

By default, no TFTP server address is specified.

If you perform the **tftp-server ip-address** command repeatedly, the last configuration overwrites the previous one.

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

Use **undo vendor-class-identifier** 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 rang 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 **voice-config** to configure specified Option 184 contents in a DHCP address pool.

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

By default, no Option 184 content is configured.

You must specify the IP address of a network calling processor first 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

The DHCP relay agent configuration is supported only on Layer 3 Ethernet ports, VLAN interfaces, and Layer 3 aggregate interfaces.

dhcp dscp (for DHCP relay agent)

Syntax

```
dhcp dscp dscp-value  
undo dhcp dscp
```

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value in DHCP packets, in the range of 0 to 63.

Description

Use **dhcp dscp** to set the DSCP value for DHCP packets sent by the DHCP relay agent.

Use **undo dhcp dscp** to restore the default.

By default, the DSCP value in DHCP packets sent by the DHCP relay agent is 56.

Examples

```
# Set the DSCP value to 30 for DHCP packets.  
<Sysname> system-view  
[Sysname] dhcp dscp 30
```

dhcp enable (for DHCP relay agent)

Syntax

```
dhcp enable  
undo dhcp enable
```

View

System view

Default level

2: System level

Parameters

None

Description

Use **dhcp enable** to enable DHCP.

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

By default, DHCP is disabled.

Enable DHCP before you perform DHCP server and relay agent configurations.

Examples

```
# Enable DHCP.  
<Sysname> system-view  
[Sysname] dhcp enable
```

dhcp relay address-check enable

Syntax

```
dhcp relay address-check enable  
undo dhcp relay address-check enable
```

View

Interface view

Default level

2: System level

Parameters

None

Description

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

Use **undo dhcp relay address-check enable** 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.

This command can be executed only on Layer 3 Ethernet ports and VLAN interfaces.

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

Use **undo dhcp relay check mac-address** 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.

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

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

Use **undo dhcp relay information circuit-id format-type** 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 only to configuring the non-user-defined circuit ID sub-option. 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 **dhcp relay information circuit-id string** to configure the padding content for the user-defined circuit ID sub-option.

Use **undo dhcp relay information circuit-id string** 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 **dhcp relay information enable** to enable the relay agent to support Option 82.

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

By default, Option 82 support is disabled on the 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

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 the access node identifier. By default, the node MAC address is used as the node identifier.

- **mac** indicates using the 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 specific character string as the node identifier, in which *node-identifier* is a string with 1 to 50 characters.

Description

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

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

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

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

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

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

This command applies only to configuring the non-user-defined remote ID sub-option. 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 **dhcp relay information remote-id string** to configure the padding content for the user-defined remote ID sub-option.

Use **undo dhcp relay information remote-id string** 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 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 the dropping of messages containing Option 82.

keep: Specifies the forwarding of messages containing Option 82 without any change.

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

Description

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

Use **undo dhcp relay information strategy** 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: Specifies the DHCP client IP address.

Description

Use **dhcp relay release ip** to request the DHCP server to release a specific 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: Specifies the client IP address for creating a static binding.

mac-address: Specifies the 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 that all client entries are to be removed.

dynamic: Specifies that dynamic client entries are to be removed.

static: Specifies that manual client entries are to be removed.

Description

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

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

Use **undo dhcp relay security refresh enable** 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: Specifies the 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. The more entries there are, the shorter the interval. The shortest interval is no less than 500 ms.

Description

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

Use **undo dhcp relay security tracker** 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 **dhcp relay server-detect** to enable unauthorized DHCP server detection.

Use **undo dhcp relay server-detect** 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 record from the request the IP addresses of all DHCP servers that ever offered IP addresses to the DHCP client and the receiving interface. Each server detected is recorded only once. The administrator can use this information from logs to check for unauthorized DHCP servers.

After information about 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: Specifies a DHCP server group by its number, in the range of 0 to 19.

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

Description

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

Use **undo dhcp relay server-group** 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 address of a DHCP server and the IP address of the 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: Specifies a DHCP server group by its number to be correlated, in the range of 0 to 19.

Description

Use **dhcp relay server-select** to correlate specified interfaces to a specific DHCP server group.

Use **undo dhcp relay server-select** 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 **dhcp select relay** 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 **undo dhcp select relay** 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 operating mode of the interface is changed from DHCP server to DHCP relay agent, the IP address leases will not be deleted. To avoid this, delete the existing IP address leases when changing the interface operating 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 about DHCP server groups that all interfaces correspond to.

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

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp relay** 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 Command output

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 Option 82 configuration information about all interfaces.

interface *interface-type interface-number*: Displays Option 82 configuration information about a specific interface.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

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

Examples

Display Option 82 configuration information about 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 Command output

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 binding information about 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 *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp relay security** to display information about bindings of DHCP relay agents. If no parameter is specified, this command displays information about all bindings.

You must 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 *Security Configuration Guide*.

Examples

```
# Display information about all bindings.  
<Sysname> display dhcp relay security  
IP Address      MAC Address      Type      Interface  
 10.1.1.5       00e0-0000-0000  Static    Vlan2  
---  1 dhcp-security item(s) found  ---
```

Table 12 Command output

Field	Description
IP Address	Client IP address.
MAC Address	Client MAC address.
Type	Type of binding, 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 *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, a case-sensitive string of 1 to 256 characters.

Description

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

You must 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 *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 Command output

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 *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp relay security tracker** 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 information about the specified DHCP server group numbered from 0 to 19.

all: Displays information about all DHCP server groups.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp relay server-group** to display configuration information about a specific DHCP server group 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 Command output

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 by its number, in the range of 0 to 19, about display DHCP packet statistics is to be displayed.

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

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp relay statistics** to display DHCP packet statistics related to a specific DHCP server group or all DHCP server groups.

If no parameter (**server-group** and **all**) 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

```

BOOTPREREQUEST	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 by its number, in the range of 0 to 19, about which statistics is to be removed from the relay agent.

Description

Use **reset dhcp relay statistics** 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

The DHCP client configuration is supported only on Layer 3 Ethernet ports, VLAN interfaces, and Layer 3 aggregate 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 Server 2000 or Windows Server 2003.

You cannot configure an interface of an aggregation group as a DHCP client.

Only HP 5500 EI switch series support Layer 3 Ethernet port configuration.

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 for which to display DHCP client information.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp client** to display DHCP client information. If no **interface** *interface-type interface-number* is specified, this command displays DHCP client information about all interfaces.

Examples

```
# Display DHCP client information about 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 Command output

Field	Description
Vlan-interface1 DHCP client information	Information about the interface acting as the DHCP client.
Current machine state	Current state of the DHCP client: <ul style="list-style-type: none"> • 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 until the T1 (1/2 lease time) timer times out.

dhcp client dscp

Syntax

```
dhcp client dscp dscp-value
undo dhcp client dscp
```

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value in DHCP packets, in the range of 0 to 63.

Description

Use **dhcp client dscp** to set the DSCP value for DHCP packets sent by the DHCP client.

Use **undo dhcp client dscp** to restore the default.

By default, the DSCP value in DHCP packets sent by the DHCP client is 56.

Examples

```
# Set the DSCP value to 30 for DHCP packets.
<Sysname> system-view
[Sysname] dhcp client dscp 30
```

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*: Enables an interface to use its MAC address as the client ID to obtain an IP address.

Description

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

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

On the HP 5500 EI switch series, by default:

- If the device starts up with initial settings, it uses the software initial setting that an interface does not use DHCP for IP address acquisition.
- If the device starts up with default configuration file, it uses the software default setting that an interface uses its MAC address to be the client ID for IP address acquisition.

For more information about initial settings and default configuration file, see *Fundamentals Configuration Guide*.

On the HP 5500 SI switch series, by default, an interface does not use DHCP for IP address acquisition.

If no parameter is specified, the client uses a character string that comprises 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 through DHCP.

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

A DHCP snooping enabled device does not work if it is between the DHCP relay agent and DHCP server. 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 **dhcp-snooping** to enable DHCP snooping.

Use **undo dhcp-snooping** 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 *Fundamentals Configuration Guide*.

Description

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

Use **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: Specifies the refresh interval in minutes, in the range of 1 to 14400.

Description

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

Use **undo dhcp-snooping binding database update interval** 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.

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-snooping 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 **dhcp-snooping binding database update now** 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 port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

None

Description

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

Use **undo dhcp-snooping check mac-address** 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 port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

None

Description

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

Use **undo dhcp-snooping check request-message** 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 port 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 **dhcp-snooping information circuit-id format-type** to configure the code type for the non-user-defined circuit ID sub-option.

Use **undo dhcp-snooping information circuit-id format-type** 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. The private padding format supports only the hex code type.

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

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

Use **undo dhcp-snooping information circuit-id string** 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 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 port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

None

Description

Use **dhcp-snooping information enable** to configure DHCP snooping to support Option 82.

Use **undo dhcp-snooping information enable** 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 | private private | standard | verbose [ node-identifier  
{ mac | sysname | user-defined node-identifier } ] }
```

```
undo dhcp-snooping information format
```

View

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

normal: Specifies the normal padding format.

private *private*: Specifies the private padding format. The *private* value must be 1.

standard: Specifies the standard 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 specific character string as the node identifier, in which *node-identifier* is a string of 1 to 50 characters.

Description

Use **dhcp-snooping information format** to specify the padding format for Option 82.

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

Use **undo dhcp-snooping information remote-id format-type** 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. The private padding format only supports the hex code type.

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

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 port 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 **dhcp-snooping information remote-id string** to configure the padding content for the user-defined remote ID sub-option.

Use **undo dhcp-snooping information remote-id string** 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.

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-snooping 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 { append | drop | keep | replace }
```

```
undo dhcp-snooping information strategy
```

View

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

append: Forwards the message containing Option 82 after adding content to the sub-option 9 of option 82. The append strategy is supported only when the private padding format and sub-option 9 are configured. In other cases, the device forwards the message without changing Option 82.

drop: Drops the message containing Option 82.

keep: Forwards the message containing Option 82 without changing Option 82.

replace: Forwards the message containing Option 82 after replacing the original Option 82 with the one padded in specified format.

Description

Use **dhcp-snooping information strategy** to configure the handling strategy for Option 82 in requesting messages.

Use **undo dhcp-snooping information strategy** to restore the default.

By default, the handling strategy for Option 82 in requesting messages is **replace**.

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

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 information sub-option

Syntax

dhcp-snooping information [**vlan** *vlan-id*] **sub-option** *sub-option-code* [**string** *user-string*&<1-8>]

undo dhcp-snooping information [**vlan** *vlan-id*] **sub-option** *sub-option-code*

View

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

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

sub-option *sub-option-code*: Specifies the number of the sub-option. Currently, only sub-option 9 is supported.

string *user-string*&<1-8>: Configures the content of the sub-option, a case-sensitive string of 1 to 63 characters. &<1-8> represents that you can enter a maximum of 8 strings separated by spaces.

Description

Use **dhcp-snooping information sub-option** to configure a sub-option.

Use **undo dhcp-snooping information sub-option** to restore the default.

By default, no sub-option is configured.

This configuration applies to the private padding format only. To configure the private padding format, use the **dhcp-snooping information format private 1** command.

If no content is configured for sub-option 9 with the **string** *user-string* option, the primary device uses sysname and the primary address of the Loopback0 interface to pad sub-option 9 and the secondary device uses sysname to pad sub-option 9. The device configured with the **dhcp-snooping information**

strategy append command is the primary device and a device configured with some other strategy is a secondary device.

After you use the **string user-string** option to configure sub-option 9, the device uses the ASCII code type to pad the characters into sub-option 9 in the order that they are configured. When the total length of all sub-options reaches 255, the device stops padding automatically.

The sub-option 9 content configured only applies to the VLAN that is specified by the **vlan vlan-id** option. If no VLAN ID is specified, the sub-option 9 content applies to all VLANs. A VLAN prefers its own sub-option 9 content over the one configured for all VLANs.

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

Examples

```
# Configure the user-defined sub-option 9 as group001.
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp-snooping information sub-option 9 string group001
```

dhcp-snooping rate-limit

Syntax

dhcp-snooping rate-limit *rate*

undo dhcp-snooping rate-limit

View

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

rate: Maximum rate of incoming DHCP packets, ranging from 64 to 512 Kbps.

Description

Use **dhcp-snooping rate-limit** to configure the maximum rate of incoming DHCP packets.

Use **undo dhcp-snooping rate-limit** to restore the default.

By default, DHCP packet rate limit is disabled.

This command takes effect only after you enable DHCP snooping.

An interface configured with DHCP packet rate limit discards incoming DHCP packets exceeding the specified maximum rate.

If a Layer 2 Ethernet port belongs to an aggregation group, it uses the DHCP packet maximum rate configured on the corresponding Layer 2 aggregate interface.

Examples

```
# Set the maximum rate of incoming DHCP packets on Layer 2 Ethernet port GigabitEthernet 1/0/1 to 64 Kbps.
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] dhcp-snooping rate-limit 64
```

dhcp-snooping trust

Syntax

```
dhcp-snooping trust [ no-user-binding ]
```

```
undo dhcp-snooping trust
```

View

Layer 2 Ethernet port 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 **dhcp-snooping trust** to configure a port as a trusted port.

Use **undo dhcp-snooping trust** 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 make sure 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 *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp-snooping** to display DHCP snooping entries.

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 , R--Recovering
Type IP Address      MAC Address      Lease      VLAN  SVLAN  Interface
==== =====
D    10.1.1.1         00e0-fc00-0006  286       1     2     GigabitEthernet1/0/1
---  1 dhcp-snooping item(s) found  ---
```

Table 16 Command output

Field	Description
Type	Entry type: <ul style="list-style-type: none">• D—Dynamic.• S—Static. Static DHCP snooping entries are not supported.• R—The DHCP snooping entry is being restored through the DHCP snooping entry file, and the interface in the entry is invalid.
IP Address	IP address assigned to the DHCP client.
MAC Address	MAC address of the DHCP client.
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.
SVLAN	Inner VLAN tag when DHCP snooping and QinQ are both enabled or the DHCP snooping device receives a packet with two VLAN tags, or N/A.
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 *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp-snooping binding database** 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 Command output

Field	Description
File name	File name.
Update interval	Interval at which the DHCP snooping entry file is refreshed.
Latest read time	Last time when the file is read.
Latest write time	Last time when the file is written.
Status	Indicates whether the file was written successfully last time.

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 Option 82 configuration information about all Layer 2 Ethernet ports.

interface *interface-type interface-number*: Displays Option 82 configuration information about a specific interface.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp-snooping information** to display Option 82 configuration information on the DHCP snooping device.

Examples

Display Option 82 configuration information about 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
```

```
  Sub-option 9: Enabled
```

```
  User defined:
```

```
    Circuit ID: company001
```

```
    Sub-option 9 content: group1
```

```
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
```

```
    Sub-option 9: Enable
```

```
    Sub-option 9 content: group1
```

```
  VLAN 20:
```

```
    Remote ID: device001
```

```
    Sub-option 9: Enabled
```

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 a specific IRF member switch. The *slot-number* argument specifies the ID of the IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters

Description

Use **display dhcp-snooping packet statistics** 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 *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display dhcp-snooping trust** 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 GigabitEthernet 1/0/1 is trusted.

reset dhcp-snooping

Syntax

```
reset dhcp-snooping { all | ip ip-address }
```

View

User view

Default level

2: System level

Parameters

all: Clears all DHCP snooping entries.

ip *ip-address*: Clears the DHCP snooping entries of the specified IP address.

Description

Use **reset dhcp-snooping** 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

1: Monitor level

Parameters

slot *slot-number*: Clears the DHCP packet statistics on a specific IRF member switch. The *slot-number* argument specifies the ID of the IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

Description

Use **reset dhcp-snooping packet statistics** 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

BOOTP client configuration can only be used on Layer 3 Ethernet ports, Layer 3 aggregate interfaces, and 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 Server 2000 or Windows Server 2003.

You cannot configure an interface of an aggregation group as a BOOTP client.

Only HP 5500 EI switch series support Layer 3 Ethernet port configuration.

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 BOOTP client information about the interface.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display bootp client** to display related information about a BOOTP client.

- If **interface** *interface-type interface-number* is not specified, the command displays information about BOOTP clients on all interfaces.
- If **interface** *interface-type interface-number* is specified, the command displays information about the BOOTP client on the specified interface.

Examples

```
# Display related information about the BOOTP client on VLAN-interface 1.
<Sysname> display bootp client interface vlan-interface 1
Vlan-interfacel BOOTP client information:
Allocated IP: 169.254.0.2 255.255.0.0
Transaction ID = 0x3d8a7431
Mac Address 00e0-fc0a-c3ef
```

Table 18 Command output

Field	Description
Vlan-interface1 BOOTP client information	Information about the interface serving as a BOOTP client.
Allocated IP	IP address assigned to the BOOTP client.
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 **ip address bootp-alloc** to enable an interface to obtain an IP address through BOOTP.

Use **undo ip address bootp-alloc** 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 the BOOTP protocol.  
<Sysname> system-view  
[Sysname] interface vlan-interface 1  
[Sysname-Vlan-interface1] ip address bootp-alloc
```

IPv4 DNS configuration commands

Only the HP 5500 EI switches support Layer 3 Ethernet port configuration.

The term "interface" in this chapter refers to Layer 3 interfaces, including VLAN interfaces and route-mode (or Layer 3) Ethernet ports. You can set an Ethernet port to operate in route mode by using the **port link-mode route** command (see *Layer 2—LAN Switching Configuration Guide*).

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 *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display dns domain** 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 Command output

Field	Description
No	Sequence number.

Field	Description
Type	Type of domain name suffix: <ul style="list-style-type: none"> • S—A statically configured domain name suffix. • D—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 dynamic cache information about type A queries. A type A query resolves a domain name to the mapped IPv4 address.

ipv6: Displays dynamic cache information about type AAAA queries. A type AAAA query resolves a domain name to the mapped IPv6 address.

naptr: Displays dynamic cache information about NAPTR queries. A NAPTR query offers the replacement rule of a character string to convert the character string to a domain name.

srv: Displays dynamic cache information about 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 *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display dns host** to display dynamic DNS cache information.

Without any keyword, this command displays dynamic DNS cache information about all query types.

Related commands: **reset dns host**.

Examples

```
# Display dynamic DNS cache information about 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
```

Table 20 Command output

Field	Description
No	Sequence number.
Host	Domain name for query.
TTL	Time that a mapping can be stored in the cache, in seconds.
Type	Query type, IP , IPv6 , NAPTR , and SRV .
Reply Data	Reply data concerning the query type: <ul style="list-style-type: none"> • 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 *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display dns server** 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 Command output

Field	Description
DNS Server	Sequence number of the DNS server, configured automatically by the device, starting from 1.
Type	Type of domain name server: <ul style="list-style-type: none"> • S—A statically configured DNS server. • D—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 *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip host** 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 Command output

Field	Description
Host	Host name.

Field	Description
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.
Flags	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 **dns domain** to configure a domain name suffix. The system can automatically add the suffix to part of the domain name you entered for resolution.

Use **undo dns domain** 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.

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 dscp

Syntax

dns dscp *dscp-value*

undo dns dscp

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value in DNS packets, in the range of 0 to 63.

Description

Use **dns dscp** to set the DSCP value for DNS packets.

Use **undo dns dscp** to restore the default.

By default, the DSCP value in DNS packets is 0.

Examples

```
# Set the DSCP value to 30 for DNS packets.  
<Sysname> system-view  
[Sysname] dns dscp 30
```

dns proxy enable

Syntax

dns proxy enable

undo dns proxy enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **dns proxy enable** to enable DNS proxy.

Use **undo dns proxy enable** 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 **dns resolve** to enable dynamic domain name resolution.

Use **undo dns resolve** 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: Specifies the IPv4 address of the DNS server.

Description

Use **dns server** to specify a DNS server.

Use **undo dns server** to remove DNS servers.

No DNS server is specified by default.

- You can configure up to six DNS servers, including those with IPv6 addresses, in system view, and up to six DNS servers on all interfaces of a device.

- A DNS server configured in system view has a higher priority than one configured in interface view. A DNS server configured earlier has a higher priority than one configured later in the same view. A DNS server manually configured has a higher priority than one dynamically obtained through DHCP.
- 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.

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-interface2
```

dns spoofing

Syntax

dns spoofing *ip-address*

undo dns spoofing

View

System view

Default level

2: System level

Parameters

ip-address: Specifies the IP address used to spoof name query requests.

Description

Use **dns spoofing** to enable DNS spoofing.

Use **undo dns spoofing** 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 device cannot forward a DNS request, or answer the request. In this case, you can enable DNS spoofing on the device to spoof a reply with the configured IP address. Once a DNS server is reachable, the device 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: Specifies the 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: Specifies the IPv4 address of the specified host in dotted decimal notation.

Description

Use **ip host** to create a host name to IPv4 address mapping in the static resolution table.

Use **undo ip host** 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 dynamic cache information about type A queries. A type A query resolves a domain name to the mapped IPv4 address.

ipv6: Clears dynamic cache information about type AAAA queries. A type AAAA query resolves a domain name to the mapped IPv6 address.

naptr: Clears dynamic cache information about NAPTR queries. A NAPTR query offers the replacement rule of a character string to convert the character string to a domain name.

srv: Clears dynamic cache information about SRV queries. An SRV query offers the domain name of a certain service site.

Description

Use **reset dns host** to clear information about the dynamic DNS cache.

Without any keyword, this command clears dynamic DNS cache information about all query types.

Related commands: **display dns host**.

Examples

```
# Clear dynamic DNS cache information about all query types.
<Sysname> reset dns host
```

IRDP configuration commands

ip irdp

Syntax

```
ip irdp  
undo ip irdp
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **ip irdp** to enable IRDP on an interface.

Use **undo ip irdp** to disable IRDP on an interface.

IRDP is disabled on an interface by default.

IRDP configuration takes effect only when IRDP is enabled.

Examples

```
# Enable IRDP on VLAN-interface 1.  
<Sysname> system-view  
[Sysname] interface vlan-interface 1  
[Sysname-Vlan-interface1] ip irdp
```

ip irdp address

Syntax

```
ip irdp address ip-address preference  
undo ip irdp address ip-address
```

View

Interface view

Default level

2: System level

Parameters

ip-address: Specifies the proxy-advertised IP address.

preference: Specifies the preference of the proxy-advertised IP address, in the range of -2147483648 to 2147483647.

Description

Use **ip irdp address** to configure an IP address to be proxy-advertised by the interface.

Use **undo ip irdp address** to remove the proxy-advertised IP address.

Examples

```
# Specify the IP address 192.168.0.8 and its preference for VLAN-interface 1 to proxy-advertise.
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip irdp address 192.168.0.8 1600
```

ip irdp lifetime

Syntax

ip irdp lifetime *lifetime-value*

undo ip irdp lifetime

View

Interface view

Default level

2: System level

Parameters

lifetime-value: Specifies the lifetime of IP addresses advertised on the interface, in the range of 4 to 9000 seconds.

Description

Use **ip irdp lifetime** to set the lifetime of IP addresses advertised on an interface.

Use **undo ip irdp lifetime** to restore the default.

By default, the lifetime is 1800 seconds.

The lifetime of IP addresses cannot be shorter than the maximum advertising interval on an interface. Otherwise, a configuration error prompt is displayed.

Related commands: **ip irdp maxadvinterval**.

Examples

```
# Set the lifetime of IP addresses advertised on VLAN-interface 1 to 2000 seconds.
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip irdp lifetime 2000
```

ip irdp maxadvinterval

Syntax

ip irdp maxadvinterval *interval-value*

undo ip irdp maxadvinterval

View

Interface view

Default level

2: System level

Parameters

interval-value: Specifies the maximum advertising interval in seconds, in the range of 4 to 1800.

Description

Use **ip irdp maxadvinterval** to set the maximum interval for advertising RAs on an interface.

Use **undo ip irdp maxadvinterval** to restore the default.

By default, the maximum advertising interval is 600 seconds.

The maximum advertising interval must be larger than the minimum interval. If not, the minimum interval will be automatically adjusted to 75% of the maximum interval.

The maximum advertising interval cannot be longer than the lifetime of advertised IP addresses. Otherwise, the lifetime will be automatically adjusted to a value three times the maximum interval.

Related commands: **ip irdp lifetime** and **ip irdp minadvinterval**.

Examples

```
# Set the maximum advertising interval on VLAN-interface 1 to 500 seconds.
```

```
<Sysname> system-view  
[Sysname] interface vlan-interface 1  
[Sysname-Vlan-interface1] ip irdp maxadvinterval 500
```

ip irdp minadvinterval

Syntax

ip irdp minadvinterval *interval-value*

undo ip irdp minadvinterval

View

Interface view

Default level

2: System level

Parameters

interval-value: Specifies the minimum advertising interval in seconds, in the range of 3 to 1800.

Parameters

Use **ip irdp minadvinterval** to set the minimum interval for advertising RAs on an interface.

Use **undo ip irdp minadvinterval** to restore the default.

By default, the minimum interval is 450 seconds.

The minimum advertising interval must be shorter than the maximum advertising interval. Otherwise, errors occur.

Related commands: **ip irdp maxadvinterval**.

Examples

```
# Set the minimum advertising interval on VLAN-interface 1 to 400 seconds.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip irdp minadinterval 400
```

ip irdp multicast

Syntax

```
ip irdp multicast
undo ip irdp multicast
```

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **ip irdp multicast** to specify the multicast address 224.0.0.1 as the destination IP address of RAs sent on an interface.

Use **undo ip irdp multicast** to restore the default.

By default, the destination IP address is 255.255.255.255.

Examples

Specify the multicast address 224.0.0.1 as the destination IP address for VLAN-interface 1 to send RAs.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip irdp multicast
```

ip irdp preference

Syntax

```
ip irdp preference preference-value
undo ip irdp preference
```

View

Interface view

Default level

2: System level

Parameters

preference-value: Specifies the preference of IP addresses advertised on an interface, in the range of -2147483648 to 2147483647. The bigger the value, the higher the preference.

Description

Use **ip irdp preference** to configure the preference of IP addresses advertised on the interface.

Use **undo ip irdp preference** to restore the default.

By default, the preference of advertised IP addresses is 0.

Examples

Configure preference 1 for IP addresses advertised on VLAN-interface 1.

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

```
[Sysname] interface vlan-interface 1
```

```
[Sysname-Vlan-interface1] ip irdp preference 1
```

IP performance optimization configuration commands

The term "interface" in this chapter refers to Layer 3 interfaces, including VLAN interfaces and route-mode (or Layer 3) Ethernet ports. You can set an Ethernet port to operate in route mode by using the **port link-mode route** command (see *Layer 2—LAN Switching Configuration Guide*).

Only the HP 5500 EI switches support configuring IP performance optimization.

Only the HP 5500 EI switches support the **vpn-instance** *vpn-instance-name* argument.

display fib

Syntax

```
display fib [ vpn-instance vpn-instance-name ] [ acl acl-number | ip-prefix ip-prefix-name ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance *vpn-instance-name*: Displays the FIB entries of the specified VPN. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Without this option specified, FIB entries of the public network are displayed.

acl *acl-number*: Displays FIB entries matching a specific 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 specific 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 *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display fib** to display FIB entries. If no parameters are specified, this command displays all FIB entries.

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 matching 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 23 Command output

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

Field	Description
Flag	Flags of routes: <ul style="list-style-type: none"> • 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 [ vpn-instance vpn-instance-name ] ip-address [ mask | mask-length ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance *vpn-instance-name*: Displays the FIB entries of the specified VPN. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Without this option specified, FIB entries of the public network are displayed.

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 *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display fib ip-address** 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 23.
```

display icmp statistics

Syntax

```
display icmp statistics [ slot slot-number ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

slot *slot-number*: Displays the ICMP statistics on a specific IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display icmp statistics** to display ICMP statistics.

Related commands: **display ip interface** and **reset ip statistics**.

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 24 Command output

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
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 request packets
mask requests	Number of input/output mask requests
mask replies	Number of input/output mask replies
information reply	Number of output 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** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

socktype *sock-type*: Displays socket information about this type. The sock type is in the range of 1 to 3, corresponding to TCP, UDP, and raw IP.

task-id: Displays socket information about this task. Task ID is in the range of 1 to 255.

socket-id: Displays information about the socket. Socket ID is in the range of 0 to 3072.

slot slot-number: Displays socket information on a specific IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip socket** to display socket information.

Examples

```
# Display TCP socket information.
```

```
<Sysname> display ip socket
SOCK_STREAM:
Task = VTYP(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 SO_SENDVFNID(0),
socket state = SS_PRIV SS_ASYNC

Task = VTYP(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_OOBNLINE SO_REUSEPORT SO_SETKEEPALIVE,
socket state = SS_ISCONNECTED SS_PRIV SS_ASYNC

Task = VTYP(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_OOBNLINE 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_SENDVFNID(0),
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_SENDVFNID(0),
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_SENDVFNID(0),
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 25 Command output

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 (available only for a 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 | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

slot *slot-number*: Displays the IP packet statistics on a specific IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display ip statistics** to display statistics of IP packets.

Related commands: **display ip interface** and **reset ip statistics**.

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 26 Command output

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

Field	Description
	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 *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display tcp statistics** 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 27 Command output

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.

Field	Description	
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.	
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 *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display udp statistics** 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 28 Command output

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*: Specifies the ACL number, in the range of 2000 to 3999. Numbers between 2000 and 2999 are for basic ACLs, and between 3000 and 3999 are for advanced ACLs. Only directed broadcasts permitted by the ACL can be forwarded.

Description

Use **ip forward-broadcast** to enable the interface to forward directed broadcasts to a directly connected network.

Use **undo ip forward-broadcast** 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 **ip forward-broadcast** to enable the switch to receive directed broadcasts.

Use **undo ip forward-broadcast** to disable the switch from receiving directed broadcasts.

By default, the switch is disabled from receiving directed broadcast.

Examples

```
# Enable the switch to receive directed broadcasts.
```

```
<Sysname> system-view
[Sysname] ip forward-broadcast
```

ip redirects enable

Syntax

```
ip redirects enable  
undo ip redirects
```

View

System view

Default level

2: System level

Parameters

None

Description

Use **ip redirects enable** to enable sending ICMP redirection packets.

Use **undo ip redirects** to disable sending ICMP redirection packets.

This feature is disabled by default.

Examples

```
# Enable sending ICMP redirect packets.  
<Sysname> system-view  
[Sysname] ip redirects enable
```

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 **ip ttl-expires enable** to enable sending ICMP timeout packets.

Use **undo ip ttl-expires** to disable sending ICMP timeout packets.

Sending ICMP timeout packets is disabled by default.

If the feature is disabled, the device will not send TTL timeout ICMP packets, but still send "reassembly timeout" ICMP packets.

Examples

```
# Enable sending ICMP timeout packets.
```

```
<Sysname> system-view
[Sysname] ip ttl-expires enable
```

ip unreachable enable

Syntax

```
ip unreachable enable
undo ip unreachable
```

View

System view

Default level

2: System level

Parameters

None

Description

Use **ip unreachable enable** to enable sending ICMP destination unreachable packets.

Use **undo ip unreachable** to disable sending ICMP destination unreachable packets.

Sending ICMP destination unreachable packets is disabled by default.

Examples

```
# Enable sending ICMP destination unreachable packets.
<Sysname> system-view
[Sysname] ip unreachable enable
```

reset ip statistics

Syntax

```
reset ip statistics [ slot slot-number ]
```

View

User view

Default level

1: Monitor level

Parameters

slot *slot-number*: Clears the IP packet statistics on a specific IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

Description

Use **reset ip statistics** to clear statistics of IP packets.

Related commands: **display ip statistics** and **display ip interface**.

Examples

```
# Clear statistics of IP packets.  
<Sysname> reset ip statistics
```

reset tcp statistics

Syntax

```
reset tcp statistics
```

View

User view

Default level

1: Monitor level

Parameters

None

Description

Use **reset tcp statistics** 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

1: Monitor level

Parameters

None

Description

Use **reset udp statistics** to clear statistics of UDP traffic.

Examples

```
# Display statistics of UDP traffic.  
<Sysname> reset udp statistics
```

tcp path-mtu-discovery

Syntax

```
tcp path-mtu-discovery [ aging minutes | no-aging ]
```

undo tcp path-mtu-discovery

View

System view

Default level

2: System level

Parameters

aging *minutes*: Specifies the aging time of the path MTU, in the range of 10 to 30 minutes. The default aging time is 10 minutes.

no-aging: Do not age out the path MTU.

Description

Use **tcp path-mtu-discovery** to enable TCP path MTU discovery.

Use **undo tcp path-mtu-discovery** to disable TCP path MTU discovery, and disable all running path MTU timers. New TCP connections do not perform TCP path MTU discovery but existing TCP connections can still use TCP path MTU discovery.

By default, TCP path MTU discovery is disabled.

Examples

```
# Enable TCP path MTU discovery and set the path MTU age timer to 20 minutes.
```

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

```
[Sysname] tcp path-mtu-discovery aging 20
```

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: Specifies the TCP finwait timer in seconds, in the range of 76 to 3600.

Description

Use **tcp timer fin-timeout** to configure the length of the TCP finwait timer.

Use **undo tcp timer fin-timeout** to restore the default.

By default, the length of the TCP finwait timer is 675 seconds.

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: Specifies the TCP synwait timer in seconds, in the range of 2 to 600.

Description

Use **tcp timer syn-timeout** to configure the length of the TCP synwait timer.

Use **undo tcp timer syn-timeout** 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: Specifies the size of the send/receive buffer in KB, in the range of 1 to 32.

Description

Use **tcp window** to configure the size of the TCP send/receive buffer.

Use **undo tcp window** 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 about forwarded UDP packets on a specific interface.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display udp-helper server** to display information about forwarded UDP packets on the specified interface or all interfaces.

If *interface-type interface-number* is not specified, this command displays information about forwarded UDP packets on all interfaces.

Examples

```
# Display information about forwarded UDP packets on the interface VLAN-interface 1.
<Sysname> display udp-helper server interface vlan-interface 1
Interface name          Server VPN          Server address  Packets
Vlan1                   20.1.1.1           20.1.1.1       0
```

The output shows that the destination server corresponding to the interface VLAN-interface 1 is in the public network, the IP address of the destination server is 20.1.1.1, and that no packets are forwarded to the destination server.

reset udp-helper packet

Syntax

```
reset udp-helper packet
```

View

User view

Default level

1: Monitor level

Parameters

None

Description

Use **reset udp-helper packet** to clear the statistics of forwarded UDP packets.

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 **udp-helper enable** to enable UDP helper. A device enabled with UDP helper functions as a relay agent that converts UDP broadcast packets into unicast packets and forwards them to a specific destination server.

Use **undo udp-helper enable** 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: Specifies the 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 **udp-helper port** to enable the forwarding of packets with the specified UDP port number.

Use **undo udp-helper port** to remove the configured UDP port numbers.

By default, no UDP port number is specified.

You can configure up to 256 UDP ports on a device.

All of the specified UDP port numbers will 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 [**vpn-instance** *vpn-instance-name*] *ip-address*

undo udp-helper server [[**vpn-instance** *vpn-instance-name*] *ip-address*]

View

Interface view

Default level

2: System level

Parameters

vpn-instance *vpn-instance-name*: Specifies the name of a MPLS L3VPN, a case-sensitive string of 1 to 31 characters. Without this option specified, the command indicates that the destination server is in the public network. This keyword and argument combination is available only on the HP 5500 EI series switches.

ip-address: Specifies the IP address of the destination server, in dotted decimal notation.

Description

Use **udp-helper server** to specify the destination server to which UDP packets are forwarded.

Use **undo udp-helper server** 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 in the public network as 192.1.1.2 on the 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

The term *interface* in this document refers to Layer 3 interfaces, including VLAN interfaces and route-mode (or Layer 3) Ethernet ports. You can set an Ethernet port to operate in route mode by using the **port link-mode route** command (see *Layer 2—LAN Switching Configuration Guide*).

Only the HP 5500 EI switches support Layer 3 Ethernet port configuration.

Only the HP 5500 EI switches support the **vpn-instance** *vpn-instance-name* argument.

display ipv6 fib

Syntax

```
display ipv6 fib [ vpn-instance vpn-instance-name ] [ acl6 acl6-number | ipv6-prefix ipv6-prefix-name ]  
[ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance *vpn-instance-name*: Displays the IPv6 FIB entries of the specified MPLS L3VPN. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Without this option specified, the **display ipv6 fib** command displays the IPv6 FIB entries of the public network.

acl6 *acl6-number*: Displays the IPv6 FIB entries permitted by a specific ACL. The ACL number is in the range of 2000 to 2999. If the specified ACL does not exist, all IPv6 FIB entries are displayed.

ipv6-prefix *ipv6-prefix-name*: Displays the IPv6 FIB entries matching a specific prefix list. The *ipv6-prefix-name* argument is a case-sensitive string of 1 to 19 characters. If the specified prefix list does not exist, all IPv6 FIB entries are displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 fib** 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                               Token          : 0
Interface        :      InLoopBack0

```

Table 29 Command output

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: <ul style="list-style-type: none"> • U—Usable route • G—Gateway route • H—Host route • B—Black hole route • D—Dynamic route • S—Static route
Label	Label
Token	LSP index number
Interface	Outgoing interface

display ipv6 fib *ipv6-address*

Syntax

```

display ipv6 fib [ vpn-instance vpn-instance-name ] ipv6-address [ prefix-length ] [ | { begin | exclude | include } regular-expression ]

```

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance *vpn-instance-name*: Displays the IPv6 FIB entries for a specific MPLS L3VPN. The *vpn-instance-name* argument is case-sensitive string of 1 to 31 characters. Without this option specified, the **display ipv6 fib *ipv6-address*** command displays IPv6 FIB entries on the public network and all private networks.

ipv6-address: Specifies the destination IPv6 address.

prefix-length: Specifies the Prefix length of the destination IPv6 address, in the range of 0 to 128.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 fib** *ipv6-address* to display the IPv6 FIB entry of the specified destination IPv6 address.

Without the *prefix-length* argument specified, this command displays the matching IPv6 FIB entry with the longest prefix.

With the *prefix-length* argument specified, this command displays the IPv6 FIB entry exactly matching the specified destination IPv6 address and prefix length.

Examples

Display the matching IPv6 FIB entry with the longest prefix.

```
<Sysname> display ipv6 fib ::1
```

Flag:

U:Useable G:Gateway H:Host B:Blackhole D:Dynamic S:Static

```
Destination:      ::1                               PrefixLength : 128
NextHop          :   ::1                               Flag          : HU
Label           :   NULL                               Token         : 0
Interface       :   InLoopBack0
```

Table 30 Command output

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: <ul style="list-style-type: none">• U—Usable route.• G—Gateway route.• H—Host route.• B—Black hole route.• D—Dynamic route.• S—Static route.
Label	Label.
Token	LSP index number.
Interface	Outgoing interface.

display ipv6 interface

Syntax

```
display ipv6 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.

brief: Displays brief IPv6 information about an interface.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 interface** to display IPv6 information about an interface.

- If *interface-type interface-number* is not specified, this command displays IPv6 information about all interfaces.
- If only *interface-type* is specified, this command displays IPv6 information about the interfaces of the specified type.
- If *interface-type interface-number* is specified, this command displays IPv6 information about the specified interface. If the **brief** keyword is also specified, this command displays brief IPv6 information about the interface.

Examples

```
# Display IPv6 information about VLAN-interface 2.
<Sysname> display ipv6 interface vlan-interface 2
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 31 Command output

Field	Description
Vlan-interface2 current state	Physical state of the interface: <ul style="list-style-type: none"> • Administratively DOWN—The VLAN interface is administratively down. The interface is shut down by using the shutdown command. • DOWN—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—The administrative and physical states of the VLAN interface are both up.
Line protocol current state	Link layer protocol state of the interface: <ul style="list-style-type: none"> • DOWN—The link layer protocol state of the VLAN interface is down. • UP—The link layer protocol state of the VLAN interface is up.

Field	Description
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 addresses 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)	Addresses of multicast groups that the interface has joined.
MTU	Maximum transmission unit of the interface.
ND DAD is enabled, number of DAD attempts	<p>Whether Duplicate Address Detection (DAD) is enabled. In this example, DAD is enabled.</p> <ul style="list-style-type: none"> 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.
OutFragFails	Packets failed in fragmentation on the outbound interface.
InUnknownProtos	Received IPv6 packets with unknown or unsupported protocol type.

Field	Description
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 path MTU.
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 brief IPv6 information about all interfaces.

```
<Sysname> display ipv6 interface brief
*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 32 Command output

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: <ul style="list-style-type: none"> • *down—The VLAN interface is administratively down. The interface is shut down using the shutdown command. • down—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—The administrative and physical states of the VLAN interface are both up.
Protocol	Link layer protocol state of the interface: <ul style="list-style-type: none"> • down—The network layer protocol state of the VLAN interface is down. • up—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 *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 nd snooping** to display ND snooping entries.

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 33 Command output

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, 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 } [ verbose ] [ | { begin | exclude | include }
regular-expression ]

```

View

Any view

Default level

1: Monitor level

Parameters

ipv6-address: Specifies the IPv6 address whose neighbor information is to be displayed.

all: Displays information about all neighbors, including neighbors acquired dynamically and configured statically on the public network and all private networks.

dynamic: Displays information about all neighbors acquired dynamically.

static: Displays information about all neighbors configured statically.

slot *slot-number*: Displays the neighbor information on a specific IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

interface *interface-type interface-number*: Displays information about the neighbors of a specific interface.

vlan *vlan-id*: Displays information about the neighbors of a specific VLAN whose ID ranges from 1 to 4094.

verbose: Displays detailed information about neighbors. This keyword is available only on the HP 5500 EI series switches.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 neighbors** 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    -
```

Display detailed information about all neighbors.

```
<Sysname> display ipv6 neighbors all verbose
                                Type: S-Static   D-Dynamic

IPv6 Address      : FE80::200:5EFF:FE32:B800
Link-layer        : 0000-5e32-b800      VID : N/A      Interface   : GE1/0/1
State             : REACH                Type: S        Age          : -
Vpn-instance      : vpn1
```

Table 34 Command output

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: <ul style="list-style-type: none"> • INCOMP—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 device will not verify the reachability any longer unless data is sent to the neighbor. • DELAY—The reachability of the neighbor is unknown. The device sends an NS message after a delay. • PROBE—The reachability of the neighbor is unknown. The device sends an NS message to verify the reachability of the neighbor.
Type	Type of neighbor information, including static configuration (represented by S) and dynamic acquisition (represented by D).

Field	Description
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 pound sign (#) is displayed (for a neighbor acquired dynamically).
Vpn-instance	Name of a VPN. [No Vrf] indicates no VPN is configured.

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 on a specific IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

interface interface-type interface-number: Displays the total number of neighbor entries of a specific interface.

vlan vlan-id: Displays the total number of neighbor entries of a specific VLAN whose ID ranges from 1 to 4094.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 neighbors count** 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 neighbors vpn-instance (available only on the HP 5500 EI)

Syntax

```
display ipv6 neighbors vpn-instance vpn-instance-name [ count ] [ | { begin | exclude | include }
regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance-name: Specifies the MPLS L3VPN for which neighbor entries are to be displayed. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters.

count: Displays the total number of neighbor entries in the specified VPN.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 neighbors vpn-instance** to display neighbor information about the specified VPN.

Examples

```
# Display neighbor information about the VPN vpn1.
```

```
<Sysname> display ipv6 neighbors vpn-instance vpn1
                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 Command output

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.

Field	Description
State	<p>State of a neighbor:</p> <ul style="list-style-type: none"> • INCOMP—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 device will not verify the reachability any longer unless data is sent to the neighbor. • DELAY—The reachability of the neighbor is unknown. The device sends an NS message after a delay. • PROBE—The reachability of the neighbor is unknown. The device sends an NS message to verify the reachability of the neighbor.
T	Type of neighbor information, which can be static (represented by S) or dynamic (represented by D).
Age	For a static entry, a hyphen (-) is displayed. For a dynamic entry, the time (in seconds) elapsed since it became reachable is displayed, and if it is never reachable, a pound sign (#) is displayed.

display ipv6 pathmtu

Syntax

```
display ipv6 pathmtu [ vpn-instance vpn-instance-name ] { ipv6-address | all | dynamic | static } [ |
{ begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

vpn-instance *vpn-instance-name*: Displays IPv6 path MTU information about the specified MPLS L3VPN. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Without this option specified, the **display ipv6 pathmtu** command displays the IPv6 path MTU information for the public network.

ipv6-address: Destination IPv6 address for which the path MTU information is to be displayed.

all: Displays all path MTU information on the public network.

dynamic: Displays all dynamic path MTU information.

static: Displays all static path MTU information.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 pathmtu** to display IPv6 path MTU information.

Examples

```
# Display all path MTU 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 Command output

Field	Description
IPv6 Destination Address	Destination IPv6 address.
ZoneID	VPN index. If the information is for the public network, this field displays 0 .
PathMTU	Path MTU value on the network path to an IPv6 address.
Age	Time for a path MTU to live. For a static path MTU, two consecutive hyphens (-) are displayed.
Type	The path MTU is dynamically negotiated or statically configured.

display ipv6 socket

Syntax

```
display ipv6 socket [ socket-type socket-type ] [ task-id socket-id ] [ slot slot-number ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

socket-type *socket-type*: Displays socket information about this type. The socket type is in the range of 1 to 3. The value 1 represents a TCP socket, value 2 a UDP socket, and value 3 a raw socket.

task-id: Displays socket information about the task. The task ID is in the range of 1 to 255.

socket-id: Displays information about the socket. The socket ID is in the range of 0 to 3072.

slot *slot-number*: Displays the socket information on a specific IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 socket** to display socket information.

With no parameter specified, this command displays information about all sockets. With only the socket type specified, the command displays information about sockets of the specified type. With the socket type, task ID and socket ID specified, the command displays information about the specified socket.

Examples

Display information about 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 SO_SENDVFNID,
socket state = SS_PRIV SS_ASYNC

Task = VTYD(14), socketid = 3, Proto = 6,
LA = ::->23, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT SO_SENDVFNID,
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 Command output

Field	Description
SOCK_STREAM	TCP socket.
SOCK_DGRAM	UDP socket.

Field	Description
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: <ul style="list-style-type: none"> • 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. • SO_SENDFD—Enables sending of the VPN ID.
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 the IPv6 and ICMPv6 packets statistics on a specific IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 statistics** 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
  unreachable:   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          router renumbering: 0
```

```
Send failed:
```

```
  ratelimited:   0          other errors:      0
```

```
Received packets:
```

```
Total:          0
  checksum error: 0          too short:         0
  bad code:       0
  unreachable:   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 Command output

Field	Description
IPv6 Protocol:	Statistics of IPv6 packets.
Sent packets:	Statistics of sent IPv6 packets:
Total: 0	<ul style="list-style-type: none"> • 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.
Local sent out: 0 forwarded: 0	
raw packets: 0 discarded: 0	
routing failed: 0 fragments: 0	
fragments failed: 0	
Received packets:	Statistics of received IPv6 packets:
Total: 0	<ul style="list-style-type: none"> • 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.
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:	Statistics of ICMPv6 packets.

Field	Description
<p>Sent packets:</p> <p>Total: 0</p> <p>unreached: 0 too big: 0</p> <p>hopcount exceeded: 0 reassembly timeout: 0</p> <p>parameter problem: 0</p> <p>echo request: 0 echo replied: 0</p> <p>neighbor solicit: 0 neighbor advert: 0</p> <p>router solicit: 0 router advert: 0</p> <p>redirected: 0 router renumbering: 0</p> <p>Send failed:</p> <p>ratelimited: 0 other errors: 0</p>	<p>Statistics of sent ICMPv6 packets:</p> <ul style="list-style-type: none"> • 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 router renumber (RR) packets. • Number of packets failing to be sent due to rate limitation. • Number of packets with other errors.
<p>Received packets:</p> <p>Total: 0</p> <p>checksum error: 0 too short: 0</p> <p>bad code: 0</p> <p>unreached: 0 too big: 0</p> <p>hopcount exceeded: 0 reassembly timeout: 0</p> <p>parameter problem: 0 unknown error type: 0</p> <p>echo request: 0 echo replied: 0</p> <p>neighbor solicit: 0 neighbor advert: 0</p> <p>router solicit: 0 router advert: 0</p> <p>redirected: 0 router renumbering: 0</p> <p>unknown info type: 0</p> <p>Deliver failed:</p> <p>bad length: 0 ratelimited: 0</p>	<p>Statistics of received ICMPv6 packets:</p> <ul style="list-style-type: none"> • 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 RR packets. • 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 *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display tcp ipv6 statistics** 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 Command output

Field	Description
Received packets:	Statistics of received packets:
Total: 0	<ul style="list-style-type: none"> Total number of received packets
packets in sequence: 0 (0 bytes)	<ul style="list-style-type: none"> Number of packets received in sequence
window probe packets: 0	<ul style="list-style-type: none"> Number of window probe packets
window update packets: 0	<ul style="list-style-type: none"> Number of window size update packets
checksum error: 0	<ul style="list-style-type: none"> Number of packets with checksum errors
offset error: 0	<ul style="list-style-type: none"> Number of packets with offset errors
short error: 0	<ul style="list-style-type: none"> Number of packets whose total length is less than specified by the packet header
duplicate packets: 0 (0 bytes), partially duplicate packets: 0 (0 bytes)	<ul style="list-style-type: none"> Number of duplicate packets Number of partially duplicate packets
out-of-order packets: 0 (0 bytes)	<ul style="list-style-type: none"> Number of out-of-order packets
packets with data after window: 0 (0 bytes)	<ul style="list-style-type: none"> Number of packets exceeding the size of the receiving window
packets after close: 0	<ul style="list-style-type: none"> Number of packets received after the connection is closed
ACK packets: 0 (0 bytes)	<ul style="list-style-type: none"> Number of ACK packets
duplicate ACK packets: 0	<ul style="list-style-type: none"> Number of duplicate ACK packets
too much ACK packets: 0	<ul style="list-style-type: none"> Number of excessive ACK packets
Sent packets:	Statistics of sent packets:
Total: 0	<ul style="list-style-type: none"> Total number of packets
urgent packets: 0	<ul style="list-style-type: none"> Number of packets containing an urgent indicator
control packets: 0 (including 0 RST)	<ul style="list-style-type: none"> Number of control packets
window probe packets: 0	<ul style="list-style-type: none"> Number of window probe packets
window update packets: 0	<ul style="list-style-type: none"> Number of window update packets
data packets: 0 (0 bytes) data	<ul style="list-style-type: none"> Number of data packets
packets retransmitted: 0 (0 bytes)	<ul style="list-style-type: none"> Number of retransmitted packets
ACK only packets: 0 (0 delayed)	<ul style="list-style-type: none"> 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 *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display tcp ipv6 status** 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.
```

```
<Sysname> display tcp ipv6 status
```

```
*: TCP6 MD5 Connection
```

```
TCP6CB      Local Address      Foreign Address      State
045d8074    ::->21              ::->0                  Listening
```

Table 40 Command output

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: <ul style="list-style-type: none">• 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 *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display udp ipv6 statistics** 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 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 Command output

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 **ipv6** to enable IPv6.

Use **undo ipv6** 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: Specifies the IPv6 address.

prefix-length: Specifies the prefix length of the IPv6 address, in the range of 1 to 128.

Description

Use **ipv6 address** to configure an IPv6 global unicast address for an interface.

Use **undo ipv6 address** to remove the IPv6 address from the interface.

By default, no global unicast address is configured for an interface.

Except for the link-local address automatically obtained and the link-local address generated through stateless autoconfiguration, all IPv6 addresses will be removed from the interface if the **undo ipv6 address** command is executed without any parameter specified.

Examples

```
# Set the global IPv6 unicast address of VLAN-interface 100 to 2001::1 with prefix length 64.
```

Method 1:

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1/64
```

Method 2:

```
<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 **ipv6 address anycast** to configure an IPv6 anycast address for an interface.

Use **undo ipv6 address anycast** 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 **ipv6 address auto** to enable the stateless address autoconfiguration function on the interface. With this function enabled, the interface can automatically generate a global unicast address.

Use **undo ipv6 address auto** to disable this function.

The stateless address autoconfiguration function is disabled by default.

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 **ipv6 address auto link-local** to automatically generate a link-local address for an interface.

Use **undo ipv6 address auto link-local** to remove the automatically generated link-local address for the interface.

By default, no link-local address is configured on an interface, and a link-local address will be automatically 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 address. If you first use 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 address. If you delete the manually assigned address, the automatically generated link-local address is validated. For more information about manual 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 **ipv6 address eui-64** to configure an EUI-64 IPv6 address for an interface.

Use **undo ipv6 address eui-64** 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 is displayed by using the **display ipv6 interface** command.

The prefix length of an EUI-64 IPv6 address cannot 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 hexadecimal in the address must be FE80 to FEBF.

Description

Use **ipv6 address link-local** to configure a link-local address for the interface.

Use **undo ipv6 address link-local** 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 hoplimit-expires enable

Syntax

```
ipv6 hoplimit-expires enable
undo ipv6 hoplimit-expires
```

View

System view

Default level

2: System level

Parameters

None

Description

Use **ipv6 hoplimit-expires enable** to enable the sending of ICMPv6 Time Exceeded packets.

Use **undo ipv6 hoplimit-expires** 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 device 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 **ipv6 icmp-error** to configure the size and update period of the token bucket.

Use **undo ipv6 icmp-error** to restore the defaults.

By default, the size is 10 and the update period is 100 milliseconds. A maximum of 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 **ipv6 icmpv6 multicast-echo-reply enable** to enable replying to multicast echo requests.

Use **undo ipv6 icmpv6 multicast-echo-reply** to disable replying to multicast echo requests.

By default, the device 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 **ipv6 nd autoconfig managed-address-flag** 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 **undo ipv6 nd autoconfig managed-address-flag** 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 **ipv6 nd autoconfig other-flag** 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 **undo ipv6 nd autoconfig other-flag** 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: Specifies the 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 **ipv6 nd dad attempts** to configure the number of attempts to send an NS message for DAD.

Use **undo ipv6 nd dad attempts** 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: Specifies the 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 device is 0. The number of hops is determined by the requesting device itself.

Description

Use **ipv6 nd hop-limit** to configure the hop limit advertised by the device.

Use **undo ipv6 nd hop-limit** to restore the default hop limit.

By default, the hop limit advertised by the device is 64.

Examples

```
# Set the hop limit advertised by the device 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: Specifies the interval for retransmitting an NS message in milliseconds, in the range of 1000 to 4294967295.

Description

Use **ipv6 nd ns retrans-timer** 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 **undo ipv6 nd ns retrans-timer** to restore the default.

By default, the local interface sends NS messages at an interval of 1000 millisecond and the Retrans Timer field in the RA messages sent 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: Specifies the neighbor reachable time in milliseconds, in the range of 1 to 3600000.

Description

Use **ipv6 nd nud reachable-time** 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 **undo ipv6 nd nud reachable-time** to restore the default.

By default, the neighbor reachable time on the local interface is 30000 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 **ipv6 nd ra halt** to enable RA message suppression.

Use **undo ipv6 nd ra halt** 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: Specifies the maximum interval for advertising RA messages in seconds, in the range of 4 to 1800.

min-interval-value: Specifies the minimum interval for advertising RA messages in seconds, in the range of 3 to 1350.

Description

Use **ipv6 nd ra interval** 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 **undo ipv6 nd ra interval** to restore the default.

By default, the maximum interval between RA messages is 600 seconds, and the minimum interval is 200 seconds.

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 **ipv6 nd ra no-advlinkmtu** to turn off the MTU option in RA messages.

Use **undo ipv6 nd ra no-advlinkmtu** 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 | ipv6-prefix/prefix-length }
```

View

Interface view

Default level

2: System level

Parameters

ipv6-prefix: Specifies the IPv6 prefix.

prefix-length: Specifies the prefix length of the IPv6 address.

valid-lifetime: Specifies the valid lifetime of a prefix in seconds, in the range of 0 to 4294967295.

preferred-lifetime: Specifies the preferred lifetime of a prefix used for stateless autoconfiguration in seconds, in the range of 0 to 4294967295.

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 **ipv6 nd ra prefix** to configure the prefix information in RA messages.

Use **undo ipv6 nd ra prefix** 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 (30 days) and preferred lifetime 604800 seconds (seven 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: Specifies the router lifetime in seconds, in the range of 0 to 9000. When it is set to 0, the device does not serve as the default router.

Description

Use **ipv6 nd ra router-lifetime** to configure the router lifetime in RA messages.

Use **undo ipv6 nd ra router-lifetime** to restore the default.

By default, the router lifetime in RA messages is 1800 seconds.

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 1000 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 **ipv6 nd snooping enable** to enable ND snooping.

Use **undo ipv6 nd snooping enable** 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 **ipv6 nd snooping enable global** 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 **undo ipv6 nd snooping enable global** 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 **ipv6 nd snooping enable link-local** 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 **undo ipv6 nd snooping enable link-local** 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 port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

number: Specifies the maximum number of ND snooping entries that can be learned by the interface, in the range of 0 to 4096.

Description

Use **ipv6 nd snooping max-learning-num** to configure the maximum number of ND snooping entries that can be learned on the interface.

Use **undo ipv6 nd snooping max-learning-num** 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 port
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 **ipv6 nd snooping uplink** to configure the interface as an uplink interface and disable it from learning ND snooping entries.

Use **undo ipv6 nd snooping uplink** to restore the default.

By default, when ND snooping is enabled on the device, an interface is allowed to learn ND snooping entries.

Examples

Configure Layer 2 Ethernet port GigabitEthernet 1/0/1 as an uplink interface and disable it 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 an uplink interface and disable it 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* } [**vpn-instance** *vpn-instance-name*]

undo ipv6 neighbor *ipv6-address interface-type interface-number*

undo ipv6 neighbor *ipv6-address mac-address* { *vlan-id port-type port-number* | **interface** *interface-type interface-number* } [**vpn-instance** *vpn-instance-name*]

View

System view

Default level

2: System level

Parameters

ipv6-address: Specifies the IPv6 address of the static neighbor entry.

mac-address: Specifies the MAC address of the static neighbor entry (48 bits long, in the format of H-H-H).

vlan-id: Specifies the VLAN ID of the static neighbor entry, in the range of 1 to 4094.

port-type port-number: Specifies a Layer 2 port of the static neighbor entry by its type and number .

interface *interface-type interface-number*: Specifies a Layer 3 interface of the static neighbor entry by its type and number.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN that the static neighbor entry belongs to. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the static neighbor entry is for the public network, do not specify this option.

Description

Use **ipv6 neighbor** to configure a static neighbor entry.

Use **undo ipv6 neighbor** 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 INCOMP state. After the device obtains the corresponding Layer 2 port information, the neighbor entry will go into 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 device will relate the VLAN interface with the IPv6 address to identify the static neighbor entry uniquely and the entry will be in REACH state.

To remove 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 neighbor stale-aging

Syntax

ipv6 neighbor stale-aging *aging-time*

undo ipv6 neighbor stale-aging

View

System view

Default level

2: System level

Parameters

aging-time: Age timer for ND entries in stale state, in the range of 1 to 24 hours.

Description

Use **ipv6 neighbor stale-aging** to set the age timer for ND entries in stale state.

Use **undo ipv6 neighbor stale-aging** to restore the default.

By default, the age timer for ND entries in stale state is four hours.

Examples

```
# Set the age timer for ND entries in stale state to two hours.
<Sysname> system-view
[Sysname] ipv6 neighbor stale-aging 2
```

ipv6 neighbors max-learning-num

Syntax

ipv6 neighbors max-learning-num *number*

undo ipv6 neighbors max-learning-num

View

Layer 2 Ethernet port view, Layer 3 Ethernet port view, VLAN interface view, Layer 2 aggregate interface view, Layer 3 aggregate interface view

Default level

2: System level

Parameters

number: Maximum number of neighbors that can be dynamically learned by the interface.

- On the HP 5500 EI switch series, the *number* argument ranges from 1 to 4096.
- On the HP 5500 SI switch series, the *number* argument ranges from 1 to 1024.

Description

Use **ipv6 neighbors max-learning-num** to configure the maximum number of neighbors that can be dynamically learned on the interface.

Use **undo ipv6 neighbors max-learning-num** to restore the default.

By default, a Layer 2 interface does not limit the number of neighbors dynamically learned. A Layer 3 interface on the HP 5500 EI switch series can learn up to 4096 neighbors dynamically. A Layer 3 interface on the HP 5500 SI switch series can learn up to 1024 neighbors dynamically.

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 [**vpn-instance** *vpn-instance-name*] *ipv6-address* [*value*]

undo ipv6 pathmtu [**vpn-instance** *vpn-instance-name*] *ipv6-address*

View

System view

Default level

2: System level

Parameters

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN that the path MTU belongs to. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If the path MTU is for the public network, do not specify this option.

ipv6-address: IPv6 address.

value: Path MTU of a specific IPv6 address, in the range of 1280 to 10000 bytes.

Description

Use **ipv6 pathmtu** to configure a static path MTU for a specific IPv6 address.

Use **undo ipv6 pathmtu** to remove the path MTU configuration for a specific IPv6 address.

By default, no static path MTU is configured.

Examples

```
# Configure a static path MTU for a specific 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: Specifies the aging time for path MTU in minutes, in the range of 10 to 100.

Description

Use **ipv6 pathmtu age** to configure the aging time for a dynamic path MTU.

Use **undo ipv6 pathmtu age** to restore the default.

By default, the aging time is 10 minutes.

The aging time is invalid for a static path MTU.

Related commands: **display ipv6 pathmtu**.

Examples

```
# Set the aging time for a dynamic path MTU to 40 minutes.
```

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

```
[Sysname] ipv6 pathmtu age 40
```

ipv6 prefer temporary-address

Syntax

```
ipv6 prefer temporary-address [ valid-lifetime preferred-lifetime ]
```

```
undo ipv6 prefer temporary-address
```

View

System view

Default level

2: System level

Parameters

valid-lifetime: Specifies the valid lifetime of temporary IPv6 addresses in seconds, in the range of 600 to 4294967295. The default valid lifetime is 604800 seconds, that is, seven days.

preferred-lifetime: Specifies the preferred lifetime of temporary IPv6 addresses in seconds, in the range of 600 to 4294967295. The default valid lifetime is 86400 seconds, that is, one day.

Description

Use **ipv6 prefer temporary-address** to configure the system to generate and preferably use the temporary IPv6 address of the sending interface as the source address of the packet to be sent.

Use **undo ipv6 prefer temporary-address** to disable the system from generating temporary IPv6 addresses and remove existing temporary IPv6 addresses.

By default, the system does not generate or use any temporary IPv6 address.

- Configure the valid lifetime greater than (or equal to) the preferred lifetime.
- Enable stateless address autoconfiguration before configuring this function.
- The preferred lifetime of a temporary IPv6 address takes the value of the preferred lifetime of the address prefix, or the value of the preferred lifetime you configure for temporary IPv6 addresses minus DESYNC_FACTOR (which is a random number ranging 0 to 600, in seconds), whichever is smaller.
- The valid lifetime of a temporary IPv6 address takes the value of the valid lifetime of the address prefix, or the value of the valid lifetime you configure for temporary IPv6 addresses, whichever is smaller.

Examples

```
# Configure the system to generate and preferably use the temporary IPv6 address of the sending interface as the source address of the packet to be sent.
```

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

```
[Sysname] ipv6 prefer temporary-address
```

ipv6 unreachable enable

Syntax

```
ipv6 unreachable enable
```

```
undo ipv6 unreachable
```

View

System view

Default level

2: System level

Parameters

None

Description

Use **ipv6 unreachable enable** to enable sending of ICMPv6 destination unreachable packets.

Use **undo ipv6 unreachable** 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 unreachable enable
```

local-proxy-nd enable

Syntax

local-proxy-nd enable

undo local-proxy-nd enable

View

VLAN interface view, Layer 3 Ethernet port view

Default level

2: System level

Parameters

None

Description

Use **local-proxy-nd enable** to enable local ND proxy.

Use **undo local-proxy-nd enable** to restore the default.

By default, local ND proxy is disabled.

Examples

```
# Enable local ND proxy on VLAN-interface 100.
```

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

```
[Sysname] interface vlan-interface 100
```

```
[Sysname-Vlan-interface100] local-proxy-nd enable
```

proxy-nd enable

Syntax

proxy-nd enable

undo proxy-nd enable

View

VLAN interface view, Layer 3 Ethernet port view

Default level

2: System level

Parameters

None

Description

Use **proxy-nd enable** to enable ND proxy.

Use **undo proxy-nd enable** to restore the default.

By default, ND proxy is disabled.

Examples

```
# Enable ND proxy on VLAN-interface 100.  
<Sysname> system-view  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] proxy-nd enable
```

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 **reset ipv6 nd snooping** 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 specific interface.

slot *slot-number*: Clears dynamic neighbor information on a specific IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

static: Clears static neighbor information on all interfaces.

Description

Use **reset ipv6 neighbors** 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 GigabitEthernet 1/0/1.
```

```
<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 path MTUs.

static: Clears all static path MTUs.

dynamic: Clears all dynamic path MTUs.

Description

Use **reset ipv6 pathmtu** to clear the path MTU information.

Examples

```
# Clear all path MTUs.  
<Sysname> reset ipv6 pathmtu all
```

reset ipv6 statistics

Syntax

```
reset ipv6 statistics [ slot slot-number ]
```

View

User view

Default level

1: Monitor level

Parameters

slot *slot-number*: Clears the IPv6 and ICMPv6 packets statistics on a specific IRF member switch. The *slot-number* argument specifies the ID of an IRF member switch. The value range for the argument depends on the number of member switches and their member IDs in the IRF fabric, which you can display with the **display irf** command. On a standalone device, the *slot-number* argument specifies the ID of the device.

Description

Use **reset ipv6 statistics** 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

1: Monitor level

Parameters

None

Description

Use **reset tcp ipv6 statistics** 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

1: Monitor level

Parameters

None

Description

Use **reset udp ipv6 statistics** 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: Specifies the finwait timer for IPv6 TCP connections in seconds, in the range of 76 to 3600.

Description

Use **tcp ipv6 timer fin-timeout** to set the finwait timer for IPv6 TCP connections.

Use **undo tcp ipv6 timer fin-timeout** 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: Specifies the synwait timer for IPv6 TCP connections in seconds, in the range of 2 to 600.

Description

Use **tcp ipv6 timer syn-timeout** to set the synwait timer for IPv6 TCP connections

Use **undo tcp ipv6 timer syn-timeout** 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: Specifies the size of the IPv6 TCP send/receive buffer in KB (kilobyte), in the range of 1 to 32.

Description

Use **tcp ipv6 window** to set the size of the IPv6 TCP send/receive buffer.

Use **undo tcp ipv6 window** 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 *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 dhcp duid** 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. If no pool number is specified, this command displays all address pool information.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 dhcp pool** 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 Command output

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 specific 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 Command output

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. If no prefix pool number is specified, this command displays brief information about all prefix pools.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 dhcp prefix-pool** 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 Command output

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 DHCPv6 server information about the interface specified by interface type and number. If no interface is specified, this command displays DHCPv6 server information about all interfaces.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 dhcp server** to display DHCPv6 server information.

Examples

```
# Display DHCPv6 server information about all interfaces.
<Sysname> display ipv6 dhcp server
DHCPv6 server status: Enabled
Interface                Pool
Vlan-interface2         1
Vlan-interface3         2

# Display DHCPv6 server information about 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 Command output

Field	Description
DHCPv6 server status	DHCPv6 server status, 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 PD information about the address pool specified by the pool number.

prefix *prefix/prefix-len*: Displays PD information about 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 PD information about the prefix pool specified by the prefix pool number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 dhcp server pd-in-use** to display PD information.

The PD information generated for static prefixes is not displayed when you display PD information about 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 PD information about 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 PD information about 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 PD information about 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 Command output

Field	Description
Total number	Total number of PDs.
Prefix	Assigned IPv6 prefix.
Type	PD type: <ul style="list-style-type: none"> • 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 expires 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 expires 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 *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 dhcp server statistics** 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 Command output

Field	Description
Packets received	Number of messages received by the DHCPv6 server. The message types include: <ul style="list-style-type: none">• SOLICIT.• REQUEST.• CONFIRM.• RENEW.• REBIND.• RELEASE.• DECLINE.• INFORMATION-REQUEST.• RELAY-FORWARD.
Packets dropped	Number of packets discarded.
Packets sent	Number of messages sent out from the DHCPv6 server. The message types include: <ul style="list-style-type: none">• 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: Specifies the IPv6 address of a DNS server.

Description

Use **dns-server** to specify a DNS server for the client.

Use **undo dns-server** to remove the specified DNS server.

No DNS server address is specified by default.

You can configure multiple DNS server addresses by using the **dns-server** command repeatedly.

The precedence of the specified DNS servers depends on the configuration sequence. The formerly specified DNS server takes precedence over the latter one.

NOTE:

You can configure up to eight DNS servers in an address pool.

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 **domain-name** to configure the domain name for the client.

Use **undo domain-name** 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 overwrites 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
```

ds-lite address

Syntax

ds-lite address *ipv6-address*

undo ds-lite address

View

DHCPv6 address pool view

Default level

2: System level

Parameters

ipv6-address: Specifies the IPv6 address of the Address Family Translation Router (AFTR).

Description

Use **ds-lite address** to specify the address of the AFTR.

Use **undo ds-lite address** to delete the address of the AFTR.

The address of the AFTR is not specified by default.

When you configure a DS-Lite tunnel, the Customer Premises Equipment (CPE) sends a DHCPv6 request to obtain the address of the AFTR. Upon receiving the request, the DHCPv6 server sends the address of the AFTR to the CPE.

You can specify only one AFTR address for an address pool. The latest setting overrides the previous one.

Examples

```
# Specify the AFTR address as 2::1.
<Sysname> system-view
[Sysname] ipv6 dhcp pool 1
[Sysname-dhcp6-pool-1] ds-lite address 2::1
```

ipv6 dhcp dscp (for DHCPv6 server)

Syntax

ipv6 dhcp dscp *dscp-value*

undo ipv6 dhcp dscp

View

System view

Default level

2: System level

Parameter

dscp-value: Specifies the DSCP value in DHCPv6 packets, in the range of 0 to 63.

Description

Use **ipv6 dhcp dscp** to set the DSCP value for the DHCPv6 packets sent by the DHCPv6 server.

Use **undo ipv6 dhcp dscp** to restore the default.

By default, the DSCP value in DHCPv6 packets is 56.

Examples

Set the DSCP value to 30 in DHCPv6 packets sent by the DHCPv6 server.

```
<Sysname> system-view  
[Sysname] ipv6 dhcp dscp 30
```

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: Specifies an address pool number.

Description

Use **ipv6 dhcp pool** 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 **undo ipv6 dhcp pool** 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: Specifies a prefix pool number.

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 **ipv6 dhcp prefix-pool** to create a prefix pool and specify the prefix and the length of the prefix assigned.

Use **undo ipv6 dhcp prefix-pool** 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 clears 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: Specifies an address pool number.

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 **ipv6 dhcp server apply pool** to apply a DHCPv6 address pool to the interface.

Use **undo ipv6 dhcp server apply pool** 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. HP recommends that you do not enable the DHCPv6 server and DHCPv6 client on the same 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.

NOTE:

Only one address pool can be applied to an interface.

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 **ipv6 dhcp server enable** to enable the DHCPv6 server.

Use **undo ipv6 dhcp server enable** to disable the DHCPv6 server.

By default, the DHCPv6 server is disabled.

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.

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 **prefix-pool** 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 **undo prefix-pool** 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

2: System level

Parameters

all: Clears all PD information.

pool *pool-number*: Clears PD information about the address pool specified by the pool number.

prefix *prefix/prefix-len*: Clears PD information about 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 **reset ipv6 dhcp server pd-in-use** to clear PD information about the DHCPv6 server.

After PD information about assigned static prefixes is removed, the PDs become ineffective static PDs.

Examples

```
# Clear all PD information.
```

```
<Sysname> reset ipv6 dhcp server pd-in-use all
```

```
# Clear PD information about the specified address pool.
```

```
<Sysname> reset ipv6 dhcp server pd-in-use pool 1
```

```
# Clear PD information about 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 **reset ipv6 dhcp server statistics** 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 **sip-server** to configure the IPv6 address or domain name of a SIP server for the client.

Use **undo sip-server** 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 last configuration does 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 **static-bind prefix** to configure a static prefix.

Use **undo static-bind prefix** 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 iaaid  
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 about the specified interface.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 dhcp relay server-address** to display information about DHCPv6 server addresses specified on the DHCPv6 relay agent.

Examples

```
# Display all 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 about VLAN-interface 2.
```

```
<Sysname> display ipv6 dhcp relay server-address interface vlan-interface 2
Interface: Vlan2
Server address(es)                Output Interface
1::1
```

Table 48 Command output

Field	Description
Interface	Interface that serves as the DHCPv6 relay agent.
Server address(es)	DHCPv6 server addresses 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 *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 dhcp relay statistics** 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 Command output

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 dscp (for DHCPv6 relay agent)

Syntax

ipv6 dhcp dscp *dscp-value*

undo ipv6 dhcp dscp

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value in DHCPv6 packets, in the range of 0 to 63.

Description

Use **ipv6 dhcp dscp** to set the DSCP value for the DHCPv6 packets sent by the DHCPv6 relay agent.

Use **undo ipv6 dhcp dscp** to restore the default.

By default, the DSCP value in DHCPv6 packets is 56.

Examples

```
# Set the DSCP value to 30 in DHCPv6 packets sent by the DHCPv6 relay agent.
```

```
<Sysname> system-view  
[Sysname] ipv6 dhcp dscp 30
```

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: Specifies the IPv6 address of the DHCPv6 server.

interface *interface-type interface-number*: Specifies an outgoing interface for DHCPv6 packets.

Description

Use **ipv6 dhcp relay server-address** to enable DHCPv6 relay agent on the interface and specify a DHCPv6 server.

Use **undo ipv6 dhcp relay server-address** 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 must specify an outgoing interface. If no outgoing interface is specified, 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 **reset ipv6 dhcp relay statistics** 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 DHCPv6 client information about a specific interface.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 dhcp client** to display DHCPv6 client information.

With no parameters specified, this command displays DHCPv6 client information about all interfaces.

Examples

```
# Display DHCPv6 client information about 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 Command output

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: <ul style="list-style-type: none">• 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 specific interface.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 dhcp client statistics** to display DHCPv6 client statistics.

With no parameters specified, DHCPv6 client statistics of all interfaces is 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 Command output

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.

ipv6 dhcp client dscp

Syntax

ipv6 dhcp client dscp *dscp-value*

undo ipv6 dhcp client dscp

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value in DHCPv6 packets, in the range of 0 to 63.

Description

Use **ipv6 dhcp client dscp** to set the DSCP value in DHCPv6 packets sent by the DHCPv6 client.

Use **undo ipv6 dhcp client dscp** to restore the default value.

By default, the DSCP value in DHCPv6 packets is 56.

Examples

```
# Set the DSCP value to 30 in the DHCPv6 packets sent by the DHCPv6 client.
```

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

```
[Sysname] ipv6 dhcp client dscp 30
```

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 specific interface.

Description

Use **reset ipv6 dhcp client statistics** to clear DHCPv6 client statistics.

With no parameters specified, DHCPv6 client statistics of all interfaces is 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 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 *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 dhcp snooping trust** 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 *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 dhcp snooping user-binding** 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 Command output

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 **ipv6 dhcp snooping enable** to enable DHCPv6 snooping globally.

Use **undo ipv6 dhcp snooping enable** 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 port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

number: Maximum number of DHCPv6 snooping entries an interface can learn, in the range of 0 to 4096.

Description

Use **ipv6 dhcp snooping max-learning-num** to configure the maximum number of DHCPv6 snooping entries an interface can learn.

Use **undo ipv6 dhcp snooping max-learning-num** 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 port 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 option interface-id enable

Syntax

ipv6 dhcp snooping option interface-id enable

undo ipv6 dhcp snooping option interface-id enable

View

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

None

Description

Use **ipv6 dhcp snooping option interface-id enable** to enable DHCPv6 snooping support for Option 18.

Use **undo ipv6 dhcp snooping option interface-id enable** to restore the default.

By default, DHCPv6 snooping support for Option 18 is disabled.

The **ipv6 dhcp snooping option interface-id enable** command is effective only when you enable DHCPv6 snooping globally in system view, and enable DHCPv6 snooping in VLAN view.

Examples

Enable DHCPv6 snooping support for Option 18.

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping enable
[Sysname] vlan 1
[Sysname-vlan1] ipv6 dhcp snooping vlan enable
[Sysname-vlan1] quit
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet 1/0/1] ipv6 dhcp snooping option interface-id enable
```

ipv6 dhcp snooping option interface-id string

Syntax

```
ipv6 dhcp snooping option interface-id string interface-id  
undo ipv6 dhcp snooping option interface-id string
```

View

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

interface-id: Specifies the DUID in user-defined Option 18, a string of 1 to 128 characters.

Description

Use **ipv6 dhcp snooping option interface-id string** to configure the DUID in Option 18.

Use **undo ipv6 dhcp snooping option interface-id string** to restore the default.

By default, the DUID in Option 18 is the DUID of the device.

Examples

```
# Specify company001 as the DUID in Option 18.  
<Sysname> system-view  
[Sysname] ipv6 dhcp snooping enable  
[Sysname] vlan 1  
[Sysname-vlan1] ipv6 dhcp snooping vlan enable  
[Sysname-vlan1] quit  
[Sysname] interface GigabitEthernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping option interface-id enable  
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping option interface-id string company001
```

ipv6 dhcp snooping option remote-id enable

Syntax

```
ipv6 dhcp snooping option remote-id enable  
undo ipv6 dhcp snooping option remote-id enable
```

View

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

None

Description

Use **ipv6 dhcp snooping option remote-id enable** to enable DHCPv6 snooping support for Option 37.

Use **undo ipv6 dhcp snooping option remote-id enable** to restore the default.

By default, DHCPv6 snooping support for Option 37 is disabled.

The **ipv6 dhcp snooping option remote-id enable** command is effective only when you enable DHCPv6 snooping globally in system view, and enable DHCPv6 snooping in VLAN view.

Examples

```
# Enable DHCPv6 snooping support for Option 37.
```

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping enable
[Sysname] vlan 1
[Sysname-vlan1] ipv6 dhcp snooping vlan enable
[Sysname-vlan1] quit
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping option remote-id enable
```

ipv6 dhcp snooping option remote-id string

Syntax

```
ipv6 dhcp snooping option remote-id string remote-id
```

```
undo ipv6 dhcp snooping option remote-id string
```

View

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

string: Specifies the DUID value in user-defined Option 37, a string of 1 to 128 characters.

Description

Use **ipv6 dhcp snooping option remote-id string** to configure the DUID in Option 37.

Use **undo ipv6 dhcp snooping option remote-id string** to restore the default.

By default, the DUID in Option 37 is the DUID of the device.

Examples

```
# Specify device001 as the DUID in Option 37.
```

```
<Sysname> system-view
[Sysname] ipv6 dhcp snooping enable
[Sysname] vlan 1
[Sysname-vlan1] ipv6 dhcp snooping vlan enable
[Sysname-vlan1] quit
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping option remote-id enable
[Sysname-GigabitEthernet1/0/1] ipv6 dhcp snooping option remote-id string device001
```

ipv6 dhcp snooping trust

Syntax

```
ipv6 dhcp snooping trust
```

undo ipv6 dhcp snooping trust

View

Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

None

Description

Use **ipv6 dhcp snooping trust** to configure a DHCPv6 trusted port.

Use **undo ipv6 dhcp snooping trust** to restore the default.

By default, all interfaces of a device with DHCPv6 snooping enabled globally are untrusted ports.

After DHCPv6 snooping is enabled, to make sure 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 port 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 **ipv6 dhcp snooping vlan enable** to enable DHCPv6 snooping for a specific VLAN.

Use **undo ipv6 dhcp snooping vlan enable** 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 **reset ipv6 dhcp snooping user-binding** to clear DHCPv6 snooping entries.

Examples

```
# Clear all DHCPv6 snooping entries.
<Sysname> reset ipv6 dhcp snooping user-binding dynamic
```

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 *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display dns ipv6 server** 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 53 Command output

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: <ul style="list-style-type: none">• S—A statically configured DNS server.• D—A DNS server obtained dynamically through DHCP or other protocols.
IPv6 Address	IPv6 address of the DNS server.

Field	Description
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 *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 host** 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 54 Command output

Field	Description
Host	Host name.
Age	Time for the entry to live. 0 is displayed in the case of static configuration.
Flags	Mapping type. Static indicates a static mapping.
IPv6Address	IPv6 address of a host.

dns ipv6 dscp

Syntax

```
dns ipv6 dscp dscp-value  
undo dns ipv6 dscp
```

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies the DSCP value in IPv6 DNS packets, in the range of 0 to 63.

Description

Use **dns ipv6 dscp** to set the DSCP value for IPv6 DNS packets.

Use **undo dns ipv6 dscp** to restore the default.

By default, the DSCP value in IPv6 DNS packets is 0.

Examples

```
# Set the DSCP value to 30 in IPv6 DNS packets.  
<Sysname> system-view  
[Sysname] dns ipv6 dscp 30
```

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: Specifies the IPv6 address of a DNS server.

interface-type interface-number: Specifies an interface by its type and number. When the IPv6 address of the DNS server is a link-local address, the two arguments must be specified.

Description

Use **dns server ipv6** to specify a DNS server.

Use **undo dns server ipv6** 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: Specifies the 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: Specifies the IPv6 address.

Description

Use **ipv6 host** to configure a mapping between host name and IPv6 address.

Use **undo ipv6 host** 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
```

Tunneling configuration commands (available only on the HP 5500 EI)

default

Syntax

default

View

Tunnel interface view

Default level

2: System level

Parameters

None

Description

CAUTION:

The **default** command might interrupt ongoing network services. Make sure you are fully aware of the impacts of this command when you perform it on a live network.

Use **default** to restore the default settings for the tunnel interface.

This command might fail to restore the default settings for some commands for reasons such as command dependencies and system restrictions. You can use the **display this** command in interface view to check for these commands, and perform their **undo** forms or follow the command reference to individually restore their default settings. If your restoration attempt still fails, follow the error message to resolve the problem.

Examples

```
# Restore the default settings of interface tunnel 1.
<Sysname> system-view
[Sysname] interface tunnel 1
[Sysname-Tunnel1] default
This command will restore the default settings. Continue? [Y/N]:y
```

description

Syntax

description *text*

undo description

View

Tunnel interface view

Default level

2: System level

Parameters

text: Description of an interface, a string of 1 to 80 characters.

Description

Use **description** to configure a description for the current interface.

Use **undo description** to restore the default.

By default, the description of a tunnel interface is **Tunnelnumber Interface**, for example, **Tunnel1 Interface**.

Related commands: **display interface tunnel**.

Examples

```
# Configure the description of interface Tunnel 1 as tunnel1.
```

```
<Sysname> system-view  
[Sysname] interface tunnel 1  
[Sysname-Tunnel1] description tunnel1
```

destination

Syntax

destination { *ip-address* | *ipv6-address* }

undo destination

View

Tunnel interface view

Default level

2: System level

Parameters

ip-address: Specifies the tunnel destination IPv4 address.

ipv6-address: Specifies the tunnel destination IPv6 address.

Description

Use **destination** to specify the destination address for the tunnel interface.

Use **undo destination** to remove the configured tunnel destination address.

By default, no tunnel destination address is configured.

The tunnel destination address must be a public address.

The tunnel destination address is the address of the peer interface receiving packets and should be configured as the source address of the peer tunnel interface.

Automatic tunnel interfaces using the same encapsulation protocol must have different source addresses. Manual tunnel interfaces using the same encapsulation protocol must have different source and destination addresses.

Related commands: **source**, **interface tunnel**, **display interface tunnel**, and **display ipv6 interface tunnel**.

Examples

```
# Configure interface VLAN-interface 100 (193.101.1.1) of Sysname 1 and interface VLAN-interface 100 (192.100.1.1) of Sysname 2 as the source and destination interfaces of a tunnel between the two devices.
```

```
<Sysname1> system-view
[Sysname1] interface tunnel 0
[Sysname1-Tunnel0] source 193.101.1.1
[Sysname1-Tunnel0] destination 192.100.1.1
<Sysname2> system-view
[Sysname2] interface tunnel 1
[Sysname2-Tunnel1] source 192.100.1.1
[Sysname2-Tunnel1] destination 193.101.1.1
```

display interface tunnel

Syntax

```
display interface [ tunnel ] [ brief [ down ] ] [ | { begin | exclude | include } regular-expression ]
display interface tunnel number [ brief ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

number: Specifies the number of a tunnel interface. With this argument, the command displays information about the specified tunnel interface.

brief: Displays brief interface information. If you do not specify this keyword, the command displays detailed interface information.

down: Displays information about interfaces in the DOWN state and the causes. If you do not specify this keyword, this command displays information about interfaces in all states.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display interface tunnel** to display information about tunnel interfaces, such as the source address, destination address, and tunnel mode.

- If you do not specify the **tunnel** keyword, this command displays information about all interfaces on the device.
- If you specify the **tunnel** keyword without the *number* argument, this command displays information about all existing tunnel interfaces.

Related commands: **interface tunnel**, **source**, **destination**, and **tunnel-protocol**.

Examples

```
# Display detailed information about interface Tunnel 0.
<Sysname> display interface tunnel 0
Tunnel0 current state: UP
Line protocol current state: UP
Description: Tunnel0 Interface
The Maximum Transmit Unit is 1476
Internet Address is 58.0.0.1/24 Primary
Encapsulation is TUNNEL, service-loopback-group ID is 1.
Tunnel source 20.0.0.2 (Vlan-interface2000), destination 20.0.0.1
Tunnel bandwidth 64 (kbps)
Tunnel protocol/transport IPv6/IP
Last clearing of counters: Never
  Last 300 seconds input:  0 bytes/sec, 0 packets/sec
  Last 300 seconds output: 28 bytes/sec, 0 packets/sec
  1847 packets input, 136451 bytes
  0 input error
  5572 packets output, 428860 bytes
  0 output error
```

Table 55 Command output

Field	Description
Tunnel0 current state	Physical state of the tunnel interface: <ul style="list-style-type: none"> • DOWN (Administratively)—The interface is administratively down. That is, the interface is shut down with the shutdown command. • DOWN—The interface is administratively up but its physical state is down. • UP—Both the administrative and physical states of the interface are up.
Line protocol current state	Link layer state of the tunnel interface: <ul style="list-style-type: none"> • DOWN—The protocol state of the interface is down. • UP—The protocol state of the interface is up.
Description	Description of the tunnel interface.
Maximum Transmit Unit	Maximum transmit unit allowed on the tunnel interface.
Internet Address	IP address of the tunnel interface. If no IP address is assigned to the interface, Internet protocol processing : disabled is displayed, which means that packets cannot be processed. Primary indicates the primary IP address of the interface. Sub indicates a secondary IP address of the interface.
Encapsulation is TUNNEL	The encapsulation protocol is tunnel.
service-loopback-group ID	ID of the service loopback group referenced by the tunnel. If service loopback group is not specified, service-loopback-group ID not set is displayed.
Tunnel source	Source address of the tunnel.

Field	Description
destination	Destination address of the tunnel.
Tunnel bandwidth	Bandwidth of the tunnel interface.
Tunnel protocol/transport	Tunnel mode and transport protocol: <ul style="list-style-type: none"> • IPv6/IP—IPv6 over IPv4 manual tunnel mode. • IPv6/IP 6to4—IPv6 over IPv4 6to4 tunnel mode. • IPv6/IP ISATAP—IPv6 over IPv4 ISATAP tunnel mode.
Last clearing of counters	Last time of clearing of counters.
Last 300 seconds input: 0 bytes/sec, 0 packets/sec	Average input rate in the last 300 seconds in bytes/sec or packets/sec.
Last 300 seconds output: 0 bytes/sec, 0 packets/sec	Average output rate in the last 300 seconds in bytes/sec or packets/sec.
packets input	Total number of input packets.
input error	Number of input error packets.
packets output	Total number of output packets.
output error	Number of output error packets.

Display brief information about interface Tunnel 0.

```
<Sysname> display interface tunnel 0 brief
```

The brief information of interface(s) under route mode:

Link: ADM - administratively down; Stby - standby

Protocol: (s) - spoofing

Interface	Link	Protocol	Main IP	Description
Tun0	UP	UP	1.1.1.1	

Display brief information about interface Tunnel 1 in DOWN state.

```
<Sysname> display interface tunnel brief down
```

The brief information of interface(s) under route mode:

Link: ADM - administratively down; Stby - standby

Interface	Link Cause
Tun1	DOWN Not connected

Table 56 Command output

Field	Description
The brief information of interface(s) under route mode	Brief information about Layer 3 interfaces.
Link: ADM - administratively down; Stby - standby	Link status. If the interface has been administratively shut down, ADM is displayed . To recover its physical state, perform the undo shutdown command.
Protocol: (s) - spoofing	(s) indicates that the network layer protocol state is UP, but the link is not available because it is an on-demand link or not present at all.
Interface	Abbreviated interface name.

Field	Description
Link	Physical link state of the interface: <ul style="list-style-type: none"> • UP—The link is up. • DOWN—The link is down. • ADM—The link has been administratively shut down. To bring it up, perform the undo shutdown command.
Protocol	Protocol state: <ul style="list-style-type: none"> • DOWN—The protocol is disabled. • UP—The protocol is enabled.
Main IP	Primary IP address of the interface.
Description	Description of the interface.
Cause	Cause of a DOWN physical link. If the port has been shut down with the shutdown command, this field displays Administratively . To bring up the port, use the undo shutdown command.

display ipv6 interface tunnel

Syntax

```
display ipv6 interface tunnel [ number ] [ brief ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

number: Displays IPv6 information on a specific tunnel interface. If no interface number is specified, IPv6 information about all tunnel interfaces will be displayed.

brief: Displays brief information about tunnel interfaces. If this keyword is not specified, detailed information and IPv6 packet statistics for tunnel interfaces are displayed.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *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, a case-sensitive string of 1 to 256 characters.

Description

Use **display ipv6 interface tunnel** to display IPv6 information for tunnel interfaces.

Examples

```
# Display detailed IPv6 information and IPv6 packet statistics for interface Tunnel 0.
<Sysname> display ipv6 interface tunnel 0
Tunnel0 current state :UP
Line protocol current state :UP
```

IPv6 is enabled, link-local address is FE80::202:201

Global unicast address(es):

3000::1, subnet is 3000::/64

Joined group address(es):

FF02::1:FF02:201

FF02::1:FF00:1

FF02::1:FF00:0

FF02::2

FF02::1

MTU is 1480 bytes

ND reachable time is 30000 milliseconds

ND retransmit interval is 1000 milliseconds

Hosts use stateless autoconfig for addresses

IPv6 Packet statistics:

InReceives:	45
InTooShorts:	0
InTruncatedPkts:	0
InHopLimitExceeds:	0
InBadHeaders:	0
InBadOptions:	0
ReasmReqds:	0
ReasmOKs:	0
InFragDrops:	0
InFragTimeouts:	0
OutFragFails:	0
InUnknownProtos:	0
InDelivers:	45
OutRequests:	45
OutForwDatagrams:	0
InNoRoutes:	0
InTooBigErrors:	0
OutFragOKs:	0
OutFragCreates:	0
InMcastPkts:	0
InMcastNotMembers:	0
OutMcastPkts:	0
InAddrErrors:	0
InDiscards:	0
OutDiscards:	0

Table 57 Command output

Field	Description
Tunnel0 current state	Physical state of the tunnel interface: <ul style="list-style-type: none"> • Administratively DOWN—The interface is administratively down. That is, the interface is shut down with the shutdown command. • DOWN—The interface is administratively up but its physical state is down. • UP—Both the administrative and physical states of the interface are up.
Line protocol current state	Link layer state of the tunnel interface: <ul style="list-style-type: none"> • DOWN—The protocol state of the interface is down. • UP—The protocol state of the interface is up.
IPv6 is enabled	IPv6 packet forwarding state of the tunnel interface. IPv6 packet forwarding is automatically enabled after an IPv6 address is assigned to the interface. IPv6 packet forwarding is enabled in the example.
link-local address	Link-local address configured for the tunnel interface.
Global unicast address(es)	Global unicast addresses configured for the tunnel interface.
Joined group address(es)	Multicast addresses of the tunnel interface.
MTU is 1480 bytes	Maximum transmission unit of the tunnel interface. It is 1480 bytes in the example.
ND reachable time	Neighbor reachable time.
ND retransmit interval	Interval for retransmitting a neighbor solicitation message.
Hosts use stateless autoconfig for addresses	Hosts use stateless autoconfiguration mode to acquire IPv6 addresses.
InReceives	All IPv6 packets received by the tunnel interface, including 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 errors.
InFragTimeouts	IPv6 fragments discarded because the interval for which they had stayed in the system buffer exceeded the specified period.
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).

Field	Description
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 received normally but discarded before they were forwarded 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 brief IPv6 information for interface Tunnel 0.

```
<Sysname> display ipv6 interface tunnel 0 brief
```

```
*down: administratively down
```

```
(s): spoofing
```

```
Interface                Physical  Protocol  IPv6 Address
Tunnel0                  up       up        3000::1
```

Table 58 Command output

Field	Description
*down	The tunnel interface is administratively down, that is, the interface is closed by using the shutdown command.
(s)	Spoofing attribute of the tunnel interface, that is, the link protocol state of the tunnel interface is up, but the link does not exist, or the link is established on demand, instead of being permanent.
Interface	Name of the tunnel interface.
Physical	Physical state of the tunnel interface: <ul style="list-style-type: none"> • *down—The interface is administratively down. That is, the interface is shut down with the shutdown command. • down—The interface is administratively up but its physical state is down. • up—Both the administrative and physical states of the interface are up.
Protocol	Link layer protocol state of the tunnel interface: <ul style="list-style-type: none"> • down—The protocol state of the interface is down. • up—The protocol state of the interface is up.

Field	Description
IPv6 Address	IPv6 address of the tunnel interface. Only the first of configured IPv6 addresses is displayed. If no address is configured for the interface, Unassigned is displayed.

interface tunnel

Syntax

```
interface tunnel number
undo interface tunnel number
```

View

System view

Default level

2: System level

Parameters

number: Specifies the number of the tunnel interface. The number of tunnels that can be created is restricted by the total number of interfaces and the memory.

Description

Use **interface tunnel** to create a tunnel interface and enter its view.

Use **undo interface tunnel** to delete a specific tunnel interface.

By default, no tunnel interface is created on the device.

Use the **interface tunnel** command to enter the interface view of a specific tunnel. If the specified tunnel interface does not exist, the system will create the interface and enter its view.

A tunnel interface number is only locally significant. Thus, the tunnel interfaces on the two ends of a tunnel can use the same or different interface numbers.

Related commands: **display interface tunnel**, **display ipv6 interface tunnel**, **source**, **destination**, and **tunnel-protocol**.

Examples

```
# Create interface Tunnel 3 and enter its view.
<Sysname> system-view
[Sysname] interface tunnel 3
[Sysname-Tunnel3]
```

mtu

Syntax

```
mtu mtu-size
undo mtu
```

View

Tunnel interface view

Default level

2: System level

Parameters

mtu-size: Specifies the MTU on the tunnel interface, in the range of 100 to 64000 bytes.

Description

Use **mtu** to set the MTU on a tunnel interface.

Use **undo mtu** to restore the default.

By default, the MTU on a tunnel interface is 64000 bytes.

Examples

```
# Set the MTU for IPv4 packets on interface Tunnel 3 to 1432 bytes.
<Sysname> system-view
[Sysname] interface tunnel 3
[Sysname-Tunnel3] mtu 1432
```

reset counters interface

Syntax

```
reset counters interface [ tunnel [ number ] ]
```

View

User view

Default level

2: System level

Parameters

number: Specifies the tunnel interface number.

Description

Use **reset counters interface** to clear the statistics of tunnel interfaces.

Before sampling network traffic within a specific period of time on an interface, you need to clear the existing statistics.

- If neither the **tunnel** keyword nor interface number is specified, this command clears the statistics of all interfaces.
- If only the **tunnel** keyword is specified, this command clears the statistics of all tunnel interfaces.
- If both the **tunnel** keyword and interface number are specified, this command clears the statistics of the specified tunnel interface.

Examples

```
# Clear the statistics of Tunnel 3.
<Sysname> reset counters interface tunnel 3
```

service-loopback-group

Syntax

```
service-loopback-group number
```


undo service-loopback-group

View

Tunnel interface view

Default level

2: System level

Parameters

number: Specifies the service loopback group ID.

Description

Use **service-loopback-group** to reference a service loopback group on the tunnel interface.

Use **undo service-loopback-group** to remove the referenced service loopback group from the tunnel interface.

By default, no service loopback group is referenced on a tunnel interface.

The service loopback group to be referenced must have been configured and have the service type set to tunnel in system view.

One tunnel interface can reference only one service loopback group.

Related commands: **display interface tunnel**; **service-loopback group** (*Layer 2—LAN Switching Command Reference*).

Examples

```
# Create service loopback group 1 of tunnel type.
```

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

```
[Sysname] service-loopback group 1 type tunnel
```

```
# Add a Layer 2 Ethernet port to service loopback group 1.
```

```
[Sysname] interface GigabitEthernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] undo stp enable
```

```
[Sysname-GigabitEthernet1/0/1] undo ndp enable
```

```
[Sysname-GigabitEthernet1/0/1] undo lldp enable
```

```
[Sysname-GigabitEthernet1/0/1] port service-loopback group 1
```

```
[Sysname-GigabitEthernet1/0/1] quit
```

```
# Reference service loopback group 1 on interface Tunnel 2.
```

```
[Sysname] interface tunnel 2
```

```
[Sysname-Tunnel2] service-loopback-group 1
```

shutdown

Syntax

```
shutdown
```

```
undo shutdown
```

View

Tunnel interface view

Default level

2: System level

Parameters

None

Description

Use **shutdown** to shut down a tunnel interface.

Use **undo shutdown** to bring up a tunnel interface.

By default, a tunnel interface is in the up state.

Examples

```
# Shut down interface Tunnel 1.
<Sysname> system-view
[Sysname] interface tunnel 1
[Sysname-Tunnel1] shutdown
```

source

Syntax

```
source { ip-address | ipv6-address | interface-type interface-number }
undo source
```

View

Tunnel interface view

Default level

2: System level

Parameters

ip-address: Specifies the tunnel source IPv4 address.

ipv6-address: Specifies the tunnel source IPv6 address.

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

Description

Use **source** to specify the source address or interface of the tunnel interface.

Use **undo source** to remove the configured source address or interface of the tunnel interface.

By default, no source address or interface is specified for the tunnel interface.

The tunnel source address or interface must be a public address or interface.

The tunnel source address is the address of the interface sending packets and should be configured as the destination address of the peer tunnel interface.

Automatic tunnel interfaces using the same encapsulation protocol must have different source addresses. Manual tunnel interfaces using the same encapsulation protocol must have different source and destination addresses.

Related commands: **destination**, **interface tunnel**, **display interface tunnel**, and **display ipv6 interface tunnel**.

Examples

```
# Set the tunnel source address to 192.100.1.1 (or the interface VLAN-interface 100) on the interface Tunnel 5.
```

```
<Sysname> system-view
[Sysname] interface tunnel 5
[Sysname-Tunnel5] source 192.100.1.1
```

Or

```
<Sysname> system-view
[Sysname] interface tunnel 5
[Sysname-Tunnel5] source vlan-interface 100
```

tunnel bandwidth

Syntax

tunnel bandwidth *bandwidth-value*

undo tunnel bandwidth

View

Tunnel interface view

Default level

2: System level

Parameters

bandwidth-value: Specifies the bandwidth value of the tunnel interface in kbps, in the range of 1 to 10000000.

Description

Use **tunnel bandwidth** to set the bandwidth of the tunnel interface.

Use **undo tunnel bandwidth** to restore the default.

By default, the bandwidth of the tunnel interface is 64 kbps.

The tunnel interface bandwidth set with the **tunnel bandwidth** command is for dynamical routing protocols to calculate the cost of a tunnel path, rather than changes the bandwidth of the tunnel interface. Refer to the bandwidth of the output interface of the packet when you set the bandwidth of the tunnel interface.

Examples

```
# Configure the bandwidth of Tunnel 0 as 100 kbps.
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] tunnel bandwidth 100
```

tunnel discard ipv4-compatible-packet

Syntax

tunnel discard ipv4-compatible-packet

undo tunnel discard ipv4-compatible-packet

View

System view

Default level

2: System level

Parameters

None

Description

Use **tunnel discard ipv4-compatible-packet** to enable dropping of IPv6 packets using IPv4-compatible IPv6 addresses.

Use **undo tunnel discard ipv4-compatible-packet** to restore the default.

By default, IPv6 packets using IPv4-compatible IPv6 addresses are not dropped.

The **tunnel discard ipv4-compatible-packet** command enables the device to check the source and destination IPv6 addresses of the de-encapsulated IPv6 packets from the tunnel and discard packets that use a source or destination IPv4-compatible IPv6 address.

Examples

```
# Enable dropping of IPv6 packets using IPv4-compatible IPv6 addresses.
```

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

```
[Sysname] tunnel discard ipv4-compatible-packet
```

tunnel-protocol

Syntax

```
tunnel-protocol ipv6-ipv4 [ 6to4 | isatap ]
```

```
undo tunnel-protocol
```

View

Tunnel interface view

Default level

2: System level

Parameters

ipv6-ipv4: Specifies the IPv6 over IPv4 manual tunnel mode.

ipv6-ipv4 6to4: Specifies the IPv6 over IPv4 6to4 tunnel mode.

ipv6-ipv4 isatap: Specifies the IPv6 over IPv4 ISATAP tunnel mode.

Description

Use **tunnel-protocol** to specify the tunnel mode for the tunnel interface.

Use **undo tunnel-protocol** to restore the default.

The default tunnel is an IPv6 manual tunnel.

You can select a tunnel mode according to the actual network topology and application. The two ends of a tunnel must have the same tunnel mode specified. Otherwise, traffic transmission may fail.

Only one automatic tunnel can be created at the start point of a tunnel.

Examples

```
# Specify the 6to4 tunnel mode for interface Tunnel 2.
```

```
<Sysname> system-view  
[Sysname] interface tunnel 2  
[Sysname-Tunnel2] tunnel-protocol ipv6-ipv4 6to4
```

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.
<i>Italic</i>	<i>Italic</i> 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

A B D E F G I L M N O P R S T U V W

A

arp check enable, 1
arp ip-conflict prompt, 10
arp max-learning-num, 1
arp send-gratuitous-arp, 9
arp static, 2
arp timer aging, 3
arp-snooping enable, 15

B

bims-server, 23
bootfile-name, 23

D

default, 229
description, 229
destination, 230
dhcp client dscp, 81
dhcp dscp (for DHCP relay agent), 57
dhcp dscp (for DHCP server), 24
dhcp enable (for DHCP relay agent), 57
dhcp enable (for DHCP server), 25
dhcp relay address-check enable, 58
dhcp relay check mac-address, 59
dhcp relay client-detect enable, 59
dhcp relay information circuit-id format-type, 60
dhcp relay information circuit-id string, 61
dhcp relay information enable, 61
dhcp relay information format, 62
dhcp relay information remote-id format-type, 63
dhcp relay information remote-id string, 63
dhcp relay information strategy, 64
dhcp relay release ip, 65
dhcp relay security refresh enable, 66
dhcp relay security static, 65
dhcp relay security tracker, 67
dhcp relay server-detect, 67
dhcp relay server-group, 68
dhcp relay server-select, 69

dhcp select relay, 70
dhcp select server global-pool, 26
dhcp server apply ip-pool, 25
dhcp server client-detect enable, 27
dhcp server detect, 27
dhcp server forbidden-ip, 28
dhcp server ip-pool, 29
dhcp server ping packets, 29
dhcp server ping timeout, 30
dhcp server relay information enable, 31
dhcp server threshold, 31
dhcp-snooping, 83
dhcp-snooping binding database filename, 83
dhcp-snooping binding database update interval, 84
dhcp-snooping binding database update now, 85
dhcp-snooping check mac-address, 85
dhcp-snooping check request-message, 86
dhcp-snooping information circuit-id format-type, 86
dhcp-snooping information circuit-id string, 87
dhcp-snooping information enable, 88
dhcp-snooping information format, 89
dhcp-snooping information remote-id format-type, 90
dhcp-snooping information remote-id string, 90
dhcp-snooping information strategy, 91
dhcp-snooping information sub-option, 92
dhcp-snooping rate-limit, 93
dhcp-snooping trust, 94
display arp, 4
display arp ip-address, 5
display arp timer aging, 6
display arp vpn-instance (available only on the HP 5500 EI), 7
display arp-snooping, 15
display bootp client, 101
display dhcp client, 79
display dhcp relay, 70
display dhcp relay information, 71
display dhcp relay security, 73

- display dhcp relay security statistics,74
- display dhcp relay security tracker,74
- display dhcp relay server-group,75
- display dhcp relay statistics,76
- display dhcp server conflict,32
- display dhcp server expired,33
- display dhcp server forbidden-ip,35
- display dhcp server free-ip,34
- display dhcp server ip-in-use,36
- display dhcp server statistics,37
- display dhcp server tree,39
- display dhcp-snooping,94
- display dhcp-snooping binding database,95
- display dhcp-snooping information,96
- display dhcp-snooping packet statistics,98
- display dhcp-snooping trust,98
- display dns domain,103
- display dns host,104
- display dns ipv6 server,225
- display dns server,105
- display fib,118
- display fib ip-address,120
- display icmp statistics,121
- display interface tunnel,231
- display ip host,106
- display ip interface,17
- display ip interface brief,19
- display ip socket,122
- display ip statistics,125
- display ipv6 dhcp client,213
- display ipv6 dhcp client statistics,215
- display ipv6 dhcp duid,192
- display ipv6 dhcp pool,192
- display ipv6 dhcp prefix-pool,194
- display ipv6 dhcp relay server-address,209
- display ipv6 dhcp relay statistics,210
- display ipv6 dhcp server,195
- display ipv6 dhcp server pd-in-use,196
- display ipv6 dhcp server statistics,198
- display ipv6 dhcp snooping trust,217
- display ipv6 dhcp snooping user-binding,218
- display ipv6 fib,142
- display ipv6 fib ipv6-address,143
- display ipv6 host,226
- display ipv6 interface,145

- display ipv6 interface tunnel,234
- display ipv6 nd snooping,149
- display ipv6 neighbors,150
- display ipv6 neighbors count,152
- display ipv6 neighbors vpn-instance (available only on the HP 5500 EI),153
- display ipv6 pathmtu,154
- display ipv6 socket,155
- display ipv6 statistics,157
- display local-proxy-arp,12
- display proxy-arp,12
- display tcp ipv6 statistics,161
- display tcp ipv6 status,163
- display tcp statistics,127
- display udp ipv6 statistics,164
- display udp statistics,129
- display udp-helper server,138
- dns domain,107
- dns dscp,107
- dns ipv6 dscp,227
- dns proxy enable,108
- dns resolve,108
- dns server,109
- dns server ipv6,227
- dns source-interface,110
- dns spoofing,110
- dns-list,40
- dns-server,200
- Documents,245
- domain-name,41
- domain-name,200
- ds-lite address,201

E

- expired,42

F

- forbidden-ip,42

G

- gateway-list,43
- gratuitous-arp-learning enable,11
- gratuitous-arp-sending enable,10

I

- interface tunnel,238
- ip address,21

- ip address bootp-alloc, [102](#)
- ip address dhcp-alloc, [81](#)
- ip address unnumbered (available only on the HP 5500 EI), [22](#)
- ip forward-broadcast (interface view), [130](#)
- ip forward-broadcast (system view), [131](#)
- ip host, [111](#)
- ip irdp, [113](#)
- ip irdp address, [113](#)
- ip irdp lifetime, [114](#)
- ip irdp maxadinterval, [114](#)
- ip irdp minadinterval, [115](#)
- ip irdp multicast, [116](#)
- ip irdp preference, [116](#)
- ip redirects enable, [132](#)
- ip ttl-expires enable, [132](#)
- ip unreachable enable, [133](#)
- ipv6, [165](#)
- ipv6 address, [166](#)
- ipv6 address anycast, [166](#)
- ipv6 address auto, [167](#)
- ipv6 address auto link-local, [168](#)
- ipv6 address eui-64, [168](#)
- ipv6 address link-local, [169](#)
- ipv6 dhcp client dscp, [216](#)
- ipv6 dhcp dscp (for DHCPv6 relay agent), [211](#)
- ipv6 dhcp dscp (for DHCPv6 server), [201](#)
- ipv6 dhcp pool, [202](#)
- ipv6 dhcp prefix-pool, [203](#)
- ipv6 dhcp relay server-address, [212](#)
- ipv6 dhcp server apply pool, [203](#)
- ipv6 dhcp server enable, [204](#)
- ipv6 dhcp snooping enable, [219](#)
- ipv6 dhcp snooping max-learning-num, [219](#)
- ipv6 dhcp snooping option interface-id enable, [220](#)
- ipv6 dhcp snooping option interface-id string, [221](#)
- ipv6 dhcp snooping option remote-id enable, [221](#)
- ipv6 dhcp snooping option remote-id string, [222](#)
- ipv6 dhcp snooping trust, [222](#)
- ipv6 dhcp snooping vlan enable, [223](#)
- ipv6 hoplimit-expires enable, [170](#)
- ipv6 host, [228](#)
- ipv6 icmp-error, [170](#)
- ipv6 icmpv6 multicast-echo-reply enable, [171](#)
- ipv6 nd autoconfig managed-address-flag, [171](#)
- ipv6 nd autoconfig other-flag, [172](#)
- ipv6 nd dad attempts, [173](#)
- ipv6 nd hop-limit, [173](#)
- ipv6 nd ns retrans-timer, [174](#)
- ipv6 nd nud reachable-time, [174](#)
- ipv6 nd ra halt, [175](#)
- ipv6 nd ra interval, [176](#)
- ipv6 nd ra no-advlinkmtu, [176](#)
- ipv6 nd ra prefix, [177](#)
- ipv6 nd ra router-lifetime, [178](#)
- ipv6 nd snooping enable, [178](#)
- ipv6 nd snooping enable global, [179](#)
- ipv6 nd snooping enable link-local, [179](#)
- ipv6 nd snooping max-learning-num, [180](#)
- ipv6 nd snooping uplink, [181](#)
- ipv6 neighbor, [181](#)
- ipv6 neighbor stale-aging, [182](#)
- ipv6 neighbors max-learning-num, [183](#)
- ipv6 pathmtu, [183](#)
- ipv6 pathmtu age, [184](#)
- ipv6 prefer temporary-address, [185](#)
- ipv6 unreachable enable, [185](#)

L

- local-proxy-arp enable, [13](#)
- local-proxy-nd enable, [186](#)

M

- mac-address station-move, [7](#)
- mtu, [238](#)

N

- nbns-list, [44](#)
- netbios-type, [45](#)
- network, [45](#)
- network ip range, [46](#)
- network mask, [47](#)
- next-server, [48](#)

O

- option, [48](#)

P

- prefix-pool, [205](#)
- proxy-arp enable, [14](#)
- proxy-nd enable, [186](#)

R

- reset arp, [8](#)
- reset arp-snooping, [16](#)
- reset counters interface, [239](#)
- reset dhcp relay statistics, [78](#)
- reset dhcp server conflict, [49](#)
- reset dhcp server ip-in-use, [49](#)
- reset dhcp server statistics, [50](#)
- reset dhcp-snooping, [99](#)
- reset dhcp-snooping packet statistics, [100](#)
- reset dns host, [112](#)
- reset ip statistics, [133](#)
- reset ipv6 dhcp client statistics, [217](#)
- reset ipv6 dhcp relay statistics, [213](#)
- reset ipv6 dhcp server pd-in-use, [206](#)
- reset ipv6 dhcp server statistics, [206](#)
- reset ipv6 dhcp snooping user-binding, [224](#)
- reset ipv6 nd snooping, [187](#)
- reset ipv6 neighbors, [187](#)
- reset ipv6 pathmtu, [188](#)
- reset ipv6 statistics, [189](#)
- reset tcp ipv6 statistics, [189](#)
- reset tcp statistics, [134](#)
- reset udp ipv6 statistics, [190](#)
- reset udp statistics, [134](#)
- reset udp-helper packet, [138](#)

S

- service-loopback-group, [239](#)
- shutdown, [240](#)
- sip-server, [207](#)
- source, [241](#)

- static-bind client-identifier, [50](#)
- static-bind ip-address, [51](#)
- static-bind mac-address, [52](#)
- static-bind prefix, [208](#)
- Subscription service, [245](#)

T

- tcp ipv6 timer fin-timeout, [190](#)
- tcp ipv6 timer syn-timeout, [191](#)
- tcp ipv6 window, [191](#)
- tcp path-mtu-discovery, [134](#)
- tcp timer fin-timeout, [135](#)
- tcp timer syn-timeout, [136](#)
- tcp window, [136](#)
- tftp-server domain-name, [53](#)
- tftp-server ip-address, [53](#)
- tunnel bandwidth, [242](#)
- tunnel discard ipv4-compatible-packet, [242](#)
- tunnel-protocol, [243](#)

U

- udp-helper enable, [139](#)
- udp-helper port, [139](#)
- udp-helper server, [140](#)

V

- vendor-class-identifier, [54](#)
- voice-config, [55](#)

W

- Websites, [245](#)