

HP 5120 EI Switch Series

Network Management and Monitoring Command Reference

Part number: 5998-1796

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

Ping, tracer, and system debugging commands.....	1
Ping and tracer commands	1
ping.....	1
ping ipv6.....	4
tracer.....	6
tracer ipv6.....	7
System debugging commands.....	8
debugging.....	8
display debugging	9
NTP configuration commands.....	11
display ntp-service sessions	11
display ntp-service status	15
display ntp-service trace	16
ntp-service access	17
ntp-service authentication enable	18
ntp-service authentication-keyid	19
ntp-service broadcast-client	20
ntp-service broadcast-server	20
ntp-service dscp	21
ntp-service in-interface disable.....	22
ntp-service max-dynamic-sessions	22
ntp-service multicast-client.....	23
ntp-service multicast-server.....	24
ntp-service reliable authentication-keyid	24
ntp-service source-interface.....	25
ntp-service unicast-peer.....	26
ntp-service unicast-server	26
Information center configuration commands.....	28
display channel	28
display info-center	29
display logbuffer.....	30
display logbuffer summary	32
display security-logfile buffer.....	33
display security-logfile summary	34
display trapbuffer	35
enable log updown	36
info-center channel name	37
info-center console channel	37
info-center enable.....	38
info-center format unicom	38
info-center logbuffer	39
info-center logfile overwrite-protection	40
info-center loghost	40
info-center loghost source.....	41
info-center monitor channel	42
info-center security-logfile alarm-threshold	43
info-center security-logfile enable.....	44
info-center security-logfile frequency	44

info-center security-logfile size-quota	45
info-center security-logfile switch-directory	45
info-center snmp channel	46
info-center source	47
info-center synchronous	48
info-center syslog channel	50
info-center timestamp	50
info-center timestamp loghost	51
info-center trapbuffer	52
reset logbuffer	53
reset trapbuffer	53
security-logfile save	54
terminal debugging	54
terminal logging	55
terminal monitor	56
terminal trapping	56
SNMP configuration commands	58
display snmp-agent community	58
display snmp-agent group	59
display snmp-agent local-engineid	60
display snmp-agent mib-view	61
display snmp-agent statistics	63
display snmp-agent sys-info	64
display snmp-agent trap queue	65
display snmp-agent trap-list	66
display snmp-agent usm-user	67
enable snmp trap updown	68
snmp-agent	69
snmp-agent calculate-password	69
snmp-agent community	71
snmp-agent group	72
snmp-agent local-engineid	73
snmp-agent log	74
snmp-agent ifmib long-ifindex enable	75
snmp-agent mib-view	76
snmp-agent packet max-size	77
snmp-agent packet response dscp	77
snmp-agent sys-info	78
snmp-agent target-host	79
snmp-agent trap enable	80
snmp-agent trap if-mib link extended	81
snmp-agent trap life	82
snmp-agent trap queue-size	83
snmp-agent trap source	84
snmp-agent usm-user { v1 v2c }	84
snmp-agent usm-user v3	86
RMON configuration commands	90
display rmon alarm	90
display rmon event	91
display rmon eventlog	92
display rmon history	94
display rmon prialarm	96
display rmon statistics	98

rmon alarm	100
rmon event	102
rmon history	103
rmon prialarm	104
rmon statistics	106
Port mirroring configuration commands	107
display mirroring-group	107
mirroring-group	108
mirroring-group mirroring-port	109
mirroring-group monitor-egress	110
mirroring-group monitor-port	111
mirroring-group reflector-port	112
mirroring-group remote-probe vlan	113
mirroring-port	114
monitor-port	115
Traffic mirroring configuration commands	116
mirror-to	116
NQA configuration commands	117
NQA client configuration commands	117
advantage-factor	117
codec-type	117
data-fill	118
data-size	119
description (any NQA operation view)	120
destination ip	120
destination port	121
display nqa history	121
display nqa reaction counters	123
display nqa result	125
display nqa statistics	129
filename	135
frequency	136
history-record enable	136
history-record keep-time	137
history-record number	137
http-version	138
mode	139
next-hop	139
nqa	140
nqa agent enable	141
nqa agent max-concurrent	141
nqa schedule	142
operation (FTP operation view)	143
operation (HTTP operation view)	143
operation interface	144
password (FTP operation view)	144
probe count	145
probe packet-interval	146
probe packet-number	147
probe packet-timeout	147
probe timeout	148
reaction checked-element icpif	149
reaction checked-element { jitter-ds jitter-sd }	150

reaction checked-element mos	151
reaction checked-element { owd-ds owd-sd }	152
reaction checked-element packet-loss	153
reaction checked-element probe-duration	154
reaction checked-element probe-fail (for trap)	156
reaction checked-element probe-fail (for trigger)	157
reaction checked-element rtt	158
reaction trap	159
resolve-target	160
route-option bypass-route	160
source interface	161
source ip	162
source port	162
statistics hold-time	163
statistics max-group	163
statistics interval	164
tos	165
ttl	165
type	166
url	167
username (FTP operation view)	167
NQA server configuration commands	168
display nqa server status	168
nqa server enable	169
nqa server tcp-connect	169
nqa server tcp-connect tos	170
nqa server udp-echo	171
nqa server udp-echo tos	171
sFlow configuration commands	173
display sflow	173
sflow agent	174
sflow collector	175
sflow counter interval	176
sflow counter collector	177
sflow flow collector	177
sflow flow max-header	178
sflow sampling-mode	178
sflow sampling-rate	179
sflow source	180
IPC configuration commands	181
display ipc channel	181
display ipc link	182
display ipc multicast-group	183
display ipc node	184
display ipc packet	184
display ipc performance	186
display ipc queue	187
ipc performance enable	188
reset ipc performance	189
PoE configuration commands	190
apply poe-profile	190
apply poe-profile interface	190
display poe device	191

display poe interface	192
display poe interface power	195
display poe pse	196
display poe pse interface	198
display poe pse interface power	199
display poe-profile	201
display poe-profile interface	202
poe disconnect	203
poe enable	203
poe legacy enable	204
poe max-power	205
poe pd-description	205
poe pd-policy priority	206
poe priority	207
poe update	208
poe utilization-threshold	208
poe-profile	209

Cluster management configuration commands..... 210

NDP configuration commands	210
display ndp	210
ndp enable	212
ndp timer aging	213
ndp timer hello	214
reset ndp statistics	214
NTDP configuration commands	215
display ntdp	215
display ntdp device-list	216
display ntdp single-device	218
ntdp enable	220
ntdp explore	220
ntdp hop	221
ntdp timer	221
ntdp timer hop-delay	222
ntdp timer port-delay	223
Cluster configuration commands	223
add-member	223
administrator-address	224
auto-build	225
black-list add-mac	227
black-list delete-mac	228
build	228
cluster	230
cluster enable	230
cluster switch-to	231
cluster-local-user	232
cluster-mac	233
cluster-mac syn-interval	233
cluster-snmp-agent community	234
cluster-snmp-agent group v3	235
cluster-snmp-agent mib-view	236
cluster-snmp-agent usm-user v3	237
delete-member	238
display cluster	238
display cluster base-topology	240

display cluster black-list	241
display cluster candidates	242
display cluster current-topology	243
display cluster members	245
ftp-server	248
holdtime	249
ip-pool	249
logging-host	250
management-vlan	251
management-vlan synchronization enable	251
nm-interface vlan-interface	252
reboot member	252
snmp-host	253
tftp-server	254
timer	254
topology accept	255
topology restore-from	256
topology save-to	256
Stack management configuration commands	258
display stack	258
stack ip-pool	259
stack role master	260
stack stack-port	261
stack switch-to	261
Support and other resources	263
Contacting HP	263
Subscription service	263
Related information	263
Documents	263
Websites	263
Conventions	264
Index	266

Ping, tracer, and system debugging commands

Ping and tracer commands

ping

Syntax

```
ping [ ip ] [ -a source-ip | -c count | -f | -h ttl | -i interface-type interface-number | -m interval | -n | -p pad | -q | -r | -s packet-size | -t timeout | -tos tos | -v ] * host
```

View

Any view

Default level

0: Visit level

Parameters

ip: Distinguishes between a destination host name and the **ping** command keywords if the name of the destination host is **i**, **ip**, **ipv** or **ipv6**. For example, you must use the command in the form of **ping ip ip** instead of **ping ip** if the destination host name is **ip**.

-a source-ip: Specifies the source IP address of an ICMP echo request (ECHO-REQUEST). It must be an IP address configured on the device. If this option is not specified, the source IP address of an ICMP echo request is the primary IP address of the outbound interface of the request.

-c count: Specifies the number of times that an ICMP echo request is sent, which is in the range of 1 to 4294967295 and defaults to 5.

-f: Discards packets larger than the MTU of a given interface, which means the ICMP echo request is not allowed to be fragmented.

-h ttl: Specifies the TTL value for an ICMP echo request, which is in the range of 1 to 255 and defaults to 255.

-i interface-type interface-number: Specifies the ICMP echo request sending interface by its type and number. If this option is not specified, the ICMP echo request sending interface is determined by searching the routing table or forwarding table according to the destination IP address.

-m interval: Specifies the interval (in milliseconds) to send an ICMP echo request, which is in the range of 1 to 65535 and defaults to 200.

- If a response from the destination is received within the timeout time, the interval to send the next echo request equals the actual response period plus the value of *interval*.
- If no response from the destination is received within the timeout time, the interval to send the next echo request equals the *timeout* value plus the value of *interval*.

-n: Disables domain name resolution for the *host* argument. When this keyword is not specified, if the host argument represents the host name of the destination, the device translates *host* into an address.

-p pad: Specifies the value of the **pad** field in an ICMP echo request, in hexadecimal format, 1 to 8 bits, in the range of 0 to ffffffff. If the specified value is less than 8 bits, 0s are added in front of the value to extend it to 8 bits. For example, if *pad* is configured as 0x2f, then the packets are padded with 0x0000002f repeatedly to make the total length of the packet meet the requirements of the device. By default, the padded value starts from 0x01 up to 0xff, where another round starts again if necessary, like 0x010203...feff01....

-q: Specifies that only statistics are displayed. Absence of this keyword indicates that all information is displayed.

-r: Specifies the recording routing information. If this keyword is not specified, routes are not recorded.

-s packet-size: Specifies the length (in bytes) of an ICMP echo request, which is in the range of 20 to 8100 and defaults to 56.

-t timeout: Specifies the timeout value (in milliseconds) of an ICMP echo reply (ECHO-REPLY). If the source does not receive an ICMP echo reply within the timeout, it considers the ICMP echo reply timed out. The value is in the range of 0 to 65535 and defaults to 2000.

-tos tos: Specifies the ToS value for an echo request, which is in the range of 0 to 255 and defaults to 0.

-v: Displays the non-ICMP echo reply received. If this keyword is not specified, the system does not display non ICMP echo reply.

host: Specifies the IP address or host name (a string of 1 to 255 characters) for the destination.

Description

Use **ping** to verify whether the destination in an IP network is reachable, and to display the related statistics.

With the **ping** command executed, the source sends an ICMP echo request to the destination:

- If the destination name is unrecognizable, the system outputs "Error: Ping: Unknown host *host-name*."
- If the source receives an ICMP echo reply from the destination within the timeout, the system outputs the related information of the reply.
- If the source does not receive an ICMP echo reply from the destination within the timeout, the system outputs "Request time out."
- To use the name of the destination host to perform the ping operation, you must configure the Domain Name System (DNS) on the device first. Otherwise, the ping operation fails.

To abort the ping operation during the execution of the command, press **Ctrl+C**.

Examples

Test whether the device with an IP address of 1.1.2.2 is reachable.

```
<Sysname> ping 1.1.2.2
PING 1.1.2.2: 56 data bytes, press CTRL_C to break
  Reply from 1.1.2.2: bytes=56 Sequence=1 ttl=254 time=205 ms
  Reply from 1.1.2.2: bytes=56 Sequence=2 ttl=254 time=1 ms
  Reply from 1.1.2.2: bytes=56 Sequence=3 ttl=254 time=1 ms
  Reply from 1.1.2.2: bytes=56 Sequence=4 ttl=254 time=1 ms
  Reply from 1.1.2.2: bytes=56 Sequence=5 ttl=254 time=1 ms

--- 1.1.2.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
```

```
0.00% packet loss
round-trip min/avg/max = 1/41/205 ms
```

The output shows the following:

- The destination is reachable.
- All ICMP echo requests sent by the source have got responses.
- The minimum time, average time, and maximum time for the packet's roundtrip time are 1 ms, 41 ms, and 205 ms respectively.

Test whether the device with an IP address of 1.1.2.2 is reachable. Only the check results are displayed.

```
<Sysname> ping -q 1.1.2.2
PING 1.1.2.2: 56 data bytes, press CTRL_C to break
```

```
--- 1.1.2.2 ping statistics ---
 5 packet(s) transmitted
 4 packet(s) received
20.00% packet loss
round-trip min/avg/max = 1/12/29 ms
```

Test whether the device with an IP address of 1.1.2.2 is reachable. The route information is displayed.

```
<Sysname> ping -r 1.1.2.2
PING 1.1.2.2: 56 data bytes, press CTRL_C to break
Reply from 1.1.2.2: bytes=56 Sequence=1 ttl=254 time=53 ms
Record Route:
 1.1.2.1
 1.1.2.2
 1.1.1.2
 1.1.1.1
Reply from 1.1.2.2: bytes=56 Sequence=2 ttl=254 time=1 ms
Record Route:
 1.1.2.1
 1.1.2.2
 1.1.1.2
 1.1.1.1
Reply from 1.1.2.2: bytes=56 Sequence=3 ttl=254 time=1 ms
Record Route:
 1.1.2.1
 1.1.2.2
 1.1.1.2
 1.1.1.1
Reply from 1.1.2.2: bytes=56 Sequence=4 ttl=254 time=1 ms
Record Route:
 1.1.2.1
 1.1.2.2
 1.1.1.2
 1.1.1.1
Reply from 1.1.2.2: bytes=56 Sequence=5 ttl=254 time=1 ms
Record Route:
 1.1.2.1
 1.1.2.2
```

```

1.1.1.2
1.1.1.1

--- 1.1.2.2 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 1/11/53 ms

```

The output shows the following:

- The destination is reachable.
- The route is 1.1.1.1 <-> {1.1.1.2; 1.1.2.1} <-> 1.1.2.2.

Table 1 Command output

Field	Description
PING 1.1.2.2	Test whether the device with IP address 1.1.2.2 is reachable.
56 data bytes	Number of data bytes in each ICMP echo request.
press CTRL_C to break	During the execution of the command, you can press Ctrl+C to abort the ping operation.
Reply from 1.1.2.2 : bytes=56 Sequence=1 ttl=255 time=1 ms	Received the ICMP reply from the device whose IP address is 1.1.2.2. If no reply is received during the timeout period, "Request time out" is displayed. <ul style="list-style-type: none"> • bytes—Indicates the number of data bytes in the ICMP reply. • Sequence—Indicates the packet sequence, used to determine whether a segment is lost, disordered or repeated. • ttl—Indicates the TTL value in the ICMP reply. • time—Indicates the response time.
Record Route:	Routers through which the ICMP echo request passed. They are displayed in inversed order. The router with a smaller distance to the destination is displayed first.
-- 1.1.2.2 ping statistics --	Statistics on data received and sent in the ping operation.
5 packet(s) transmitted	Number of ICMP echo requests sent.
5 packet(s) received	Number of ICMP echo requests received.
0.00% packet loss	Percentage of packets not responded to the total packets sent.
round-trip min/avg/max = 0/4/20 ms	Minimum/average/maximum response time, in ms. The field is not available for failed ping attempts in an IPv4 network. In an IPv6 network, however, the field is available and set to 0/0/0 ms .

ping ipv6

Syntax

```
ping ipv6 [ -a source-ipv6 | -c count | -m interval | -s packet-size | -t timeout | -tos tos ] * host [ -i interface-type interface-number ]
```

View

Any view

Default level

0: Visit level

Parameters

-a source-ipv6: Specifies the source IPv6 address of an ICMP echo request. It must be a legal IPv6 address configured on the device. If this option is not specified, the source IPv6 address of an ICMP echo request is the address of the outbound interface of the request. The address selection rule is defined by RFC 3484.

-c count: Specifies the number of times that an ICMPv6 echo request is sent, which is in the range of 1 to 4294967295 and defaults to 5.

-m interval: Specifies the interval (in milliseconds) to send an ICMPv6 echo reply, which is in the range of 1 to 65535 and defaults to 200.

- If a response from the destination is received within the timeout time, the interval to send the next echo request equals the actual response period plus the value of *interval*.
- If no response from the destination is received within the timeout time, the interval to send the next echo request equals the *timeout* value plus the value of *interval*.

-s packet-size: Specifies the length (in bytes) of an ICMPv6 echo request, which is in the range of 20 to 8100 and defaults to 56.

-t timeout: Specifies the timeout value (in milliseconds) of an ICMPv6 echo reply, which is in the range of 0 to 65535 and defaults to 2000.

-tos tos: Specifies the ToS value for an IPv6 echo request, which is in the range of 0 to 255 and defaults to 0.

host: Specifies the IPv6 address or host name of the destination, a string of 1 to 255 characters.

-i interface-type interface-number: Specifies an outbound interface by its type and number. This parameter can be used only when the destination address is the link local address and the specified outbound interface must have a link local address. For more information about the configuration of a link local address, see *Layer 3—IP Services Configuration Guide*. If this parameter is not provided, the ICMP echo request sending interface is determined by searching the routing table or forwarding table according to the destination IP address.

Description

Use **ping ipv6** to verify whether an IPv6 address is reachable, and display the corresponding statistics.

To use the name of the destination host to perform the ping ipv6 operation, you must configure DNS on the device first. Otherwise, the ping ipv6 operation fails. For more information about DNS, see *Layer 3—IP Services Configuration Guide*.

To abort the ping ipv6 operation during the execution of the command, press **Ctrl+C**.

Examples

Verify whether the IPv6 address 2001::1 is reachable.

```
<Sysname> ping ipv6 2001::1
PING 2001::2 : 56 data bytes, press CTRL_C to break
  Reply from 2001::1
    bytes=56 Sequence=1 hop limit=64 time = 62 ms
  Reply from 2001::1
    bytes=56 Sequence=2 hop limit=64 time = 26 ms
  Reply from 2001::1
```

```

bytes=56 Sequence=3 hop limit=64  time = 20 ms
Reply from 2001::1
bytes=56 Sequence=4 hop limit=64  time = 4 ms
Reply from 2001::1
bytes=56 Sequence=5 hop limit=64  time = 16 ms

--- 2001::2 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
round-trip min/avg/max = 4/25/62 ms

```

The "hop limit" field in this prompt information has the same meaning as the "ttl" field in the prompt information displayed by the IPv4 **ping** command, indicating the TTL value in the ICMPv6 echo request. For a description of other fields, see [Table 1](#).

tracert

Syntax

```
tracert [ -a source-ip | -f first-ttl | -m max-ttl | -p port | -q packet-number | -tos tos | -w timeout ] * host
```

View

Any view

Default level

0: Visit level

Parameters

-a *source-ip*: Specifies the source IP address of a tracert packet. It must be a legal IP address configured on the device. If this option is not specified, the source IP address of an ICMP echo request is the primary IP address of the outbound interface of the tracert packet.

-f *first-ttl*: Specifies the first TTL (the allowed number of hops for the first packet). It is in the range of 1 to 255 and defaults to 1, and must be less than the maximum TTL.

-m *max-ttl*: Specifies the maximum TTL, or, the maximum allowed number of hops for a packet. It is in the range of 1 to 255 and defaults to 30, and must be greater than the first TTL.

-p *port*: Specifies the UDP port number of the destination, which is in the range of 1 to 65535 and defaults to 33434.

-q *packet-number*: Specifies the number of probe packets sent each time, which is in the range of 1 to 65535 and defaults to 3.

-tos *tos*: Specifies the ToS value for a tracert packet, which is in the range of 0 to 255 and defaults to 0.

-w *timeout*: Specifies the timeout time of the reply packet of a probe packet, which is in the range of 1 to 65535 milliseconds and defaults to 5000 milliseconds.

host: Specifies the IP address or host name (a string of 1 to 255 characters) for the destination.

Description

Use **tracert** to trace the path that the packets traverse from source to destination.

In the event of network failure, you can use the **tracert** command to determine the failed nodes.

The output from the **tracert** command includes IP addresses of all the Layer 3 devices that the packets traverse from source to destination. Asterisks (* * *) are displayed if the device cannot reply with an ICMP error message (probably because the destination is unreachable or sending ICMP timeout/destination unreachable packets is disabled).

To abort the tracert operation during the execution of the command, press **Ctrl+C**.

Examples

Display the path that the packets traverse from source to destination with an IP address of 1.1.2.2.

```
<Sysname> tracert 1.1.2.2
  traceroute to 1.1.2.2(1.1.2.2) 30 hops max, 40 bytes packet, press CTRL_C to break
  1  1.1.1.2 673 ms 425 ms 30 ms
  2  1.1.2.2 580 ms 470 ms 80 ms
```

Table 2 Command output

Field	Description
traceroute to 1.1.2.2(1.1.2.2)	Display the route that the IP packets traverse from the current device to the device whose IP address is 1.1.2.2.
hops max	Maximum number of hops of the probe packets, which can be set through the -m keyword.
bytes packet	Number of bytes of a probe packet.
press CTRL_C to break	During the execution of the command, you can press Ctrl+C to abort the tracert operation.
1 1.1.1.2 673 ms 425 ms 30 ms	Probe result of the probe packets whose TTL is 1, including the IP address of the first hop and the roundtrip time of three probe packets. The number of packets that can be sent in each probe can be set through the -q keyword.

tracert ipv6

Syntax

tracert ipv6 [**-f** *first-ttl* | **-m** *max-ttl* | **-p** *port* | **-q** *packet-number* | **-tos** *tos* | **-w** *timeout*] * *host*

View

Any view

Default level

0: Visit level

Parameters

-f *first-ttl*: Specifies the first TTL, or, the allowed number of hops for the first packet. It is in the range of 1 to 255 and defaults to 1, and must be less than the maximum TTL.

-m *max-ttl*: Specifies the maximum TTL (the maximum allowed number of hops for a packet). It is in the range of 1 to 255 and defaults to 30, and must be greater than the first TTL.

-p *port*: Specifies the UDP port number of the destination, which is in the range of 1 to 65535 and defaults to 33434.

-q *packet-number*: Specifies the number of probe packets sent each time, which is in the range of 1 to 65535 and defaults to 3.

-w timeout: Specifies the timeout time of the reply packet of a probe packet, which is in the range of 1 to 65535 milliseconds and defaults to 5000 milliseconds.

host: Specifies the IPv6 address or host name of the destination, a string of 1 to 46 characters.

-tos tos: Specifies the ToS value for an IPv6 tracer packet, which is in the range of 0 to 255 and defaults to 0.

Description

Use **tracert ipv6** to view the path the IPv6 packets traverse from source to destination.

In the event of network failure, you can use this command to determine the failed nodes.

Output from the **tracert ipv6** command includes IPv6 addresses of all the Layer 3 devices the packets traverse from source to destination. Asterisks (* * *) are displayed if the device cannot reply with an ICMP error message (probably because the destination is unreachable or sending ICMP timeout/destination unreachable packets is disabled).

To abort the tracer operation during the execution of the command, press **Ctrl+C**.

Examples

View the path the packets traverse from source to destination with IPv6 address 2001::1.

```
<Sysname> tracert ipv6 2001::1
  traceroute to 2001::1 30 hops max, 60 bytes packet, press CTRL_C to break
  1  2001::1 3 ms <1 ms 19 ms
```

For a description of the fields in the output, see [Table 2](#).

System debugging commands

debugging

Syntax

```
debugging module-name [ option ]
undo debugging { all | module-name [ option ] }
```

View

User view

Default level

1: Monitor level

Parameters

all: All debugging functions.

module-name: Module name, such as arp or device. To display the current module name, use the **debugging ?** command.

option: The debugging option for a specific module. Different modules have different debugging options in terms of their number and content. To display the currently supported options, use the **debugging module-name ?** command.

Description

Use **debugging** to enable the debugging of a specific module.

Use **undo debugging** to disable the debugging of a specific module.

By default, debugging functions of all modules are disabled.

Output of the debugging information may degrade system efficiency, so you should enable the debugging of the corresponding module for diagnosing network failure, and not to enable debugging of multiple modules at the same time.

Default level describes the default level of the **debugging all** command. Different **debugging** commands may have different default levels.

Configure the **debugging**, **terminal debugging** and **terminal monitor** commands first to display detailed debugging information on the terminal. For more information about the **terminal debugging** and **terminal monitor** commands, see "[Information center configuration commands](#)."

Related commands: **display debugging**.

Examples

```
# Enable IP packet debugging.  
<Sysname> debugging ip packet
```

display debugging

Syntax

```
display debugging [ interface interface-type interface-number ] [ module-name ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

interface *interface-type interface-number*: Displays the debugging settings of the specified interface, where the *interface-type interface-number* argument represents the interface type and number.

module-name: Module name.

|: 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 debugging** to display enabled debugging functions.

Related commands: **debugging**.

Examples

```
# Display all enabled debugging functions.  
<Sysname> display debugging
```

IP packet debugging is on

NTP configuration commands

display ntp-service sessions

Syntax

display ntp-service sessions [**verbose**] [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

verbose: Displays detailed information about all NTP sessions. If you do not specify this keyword, the command only displays brief information about the NTP sessions.

|: 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 ntp-service sessions** to display information about all NTP sessions.

Examples

Display brief information about all NTP sessions.

```
<Sysname> display ntp-service sessions
      source           reference           stra reach poll  now offset  delay disper
*****
[12345]127.127.1.0      127.127.1.0           3      1   64   33   0.0   0.0   0.0
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations : 1
```

Table 3 Command output

Field	Description
source	IP address of the clock source.

Field	Description
reference	<p>Reference clock ID of the clock source:</p> <ul style="list-style-type: none"> If the reference clock is the local clock, the value of this field is related to the value of the stra field: <ul style="list-style-type: none"> When the value of the stra field is 0 or 1, this field is LOCL. When the stra field has another value, this field is the IP address of the local clock. If the reference clock is the clock of another device on the network, the value of this field is the IP address of that device.
stra	Stratum level of the clock source, which determines the clock precision. The value range is 1 to 16. The clock precision decreases from stratum 1 to stratum 16. A stratum 1 clock has the highest precision, and a stratum 16 clock is not synchronized.
reach	Reachability count of the clock source. A value of 0 indicates that the clock source is unreachable.
poll	Poll interval in seconds, namely, the maximum interval between successive NTP messages.
now	<p>Length of time from when the last NTP message was received or when the local clock was last updated to the current time.</p> <p>Time is in seconds by default. If the time length is greater than 2048 seconds, it is displayed in minutes; if greater than 300 minutes, in hours; if greater than 96 hours, in days.</p>
offset	Offset of the system clock relative to the reference clock, in milliseconds.
delay	Roundtrip delay from the local device to the clock source, in milliseconds.
disper	Maximum error of the system clock relative to the reference source.
[12345]	<ul style="list-style-type: none"> 1—Clock source selected by the switch, namely, the current reference source. 2—Stratum level of the clock source is less than or equal to 15. 3—This clock source has survived the clock selection algorithm. 4—This clock source is a candidate clock source. 5—This clock source was created by a configuration command.
Total associations	Total number of associations.

Display detailed information about all NTP sessions.

```
<Sysname> display ntp-service sessions verbose
clock source: 127.127.1.0
clock stratum: 3
clock status: configured, master, sane, valid
reference clock ID: 127.127.1.0
local mode: client, local poll: 6
peer mode: server, peer poll: 6
offset: 0.0000 ms,delay: 0.00 ms,  disper: 0.02 ms
root delay: 0.00 ms, root disper: 10.00 ms
reach: 1, sync dist: 0.010, sync state: 2
precision: 2^18, version: 3, peer interface: InLoopBack0
```

```

reftime: 10:56:22.442 UTC Jan 7 2011(CE2686D6.71484513)
orgtime: 10:56:22.442 UTC Jan 7 2011(CE2686D6.71484513)
rcvtime: 10:56:22.442 UTC Jan 7 2011(CE2686D6.7149E881)
xmttime: 10:56:22.442 UTC Jan 7 2011(CE2686D6.71464DC2)
filter delay : 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
filter offset: 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
filter disper: 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
Total associations : 1

```

Table 4 Command output

Field	Description
clock source	IP address of the clock source.
clock stratum	Stratum level of the clock source, which determines the clock precision. The value range is 1 to 16. The clock precision decreases from stratum 1 to stratum 16. A stratum 1 clock has the highest precision, and a stratum 16 clock is not synchronized.
clock status	<p>Status of the clock source corresponding to this session:</p> <ul style="list-style-type: none"> • configured—The session was created by a configuration command. • dynamic—This session is established dynamically. • master—The clock source is the primary reference source of the current system. • selected—The clock source has survived the clock selection algorithm. • candidate—The clock source is the candidate reference source. • sane—The clock source has passed the sane authentication. • insane—The clock source has failed the sane authentication. • valid—The clock source is valid, which means the clock source meet the following requirements: it has passed the authentication and is being synchronized; its stratum level is valid; and its root delay and root dispersion values are within their ranges. • invalid—The clock source is invalid. • unsynced—The clock source has not been synchronized or the value of the stratum level is invalid.
reference clock ID	<p>Reference clock ID of the clock source:</p> <ul style="list-style-type: none"> • If the reference clock is the local clock, the value of this field is related to the stratum level of the clock source: <ul style="list-style-type: none"> ◦ When the stratum level of the clock source is 0 or 1, this field is LOCL. ◦ When the stratum level of the clock source has another value, this field is the IP address of the local clock. • If the reference clock is the clock of another device on the network, the value of this field is the IP address of that device.

Field	Description
local mode	<p>Operation mode of the local device:</p> <ul style="list-style-type: none"> • unspec—The mode is unspecified. • active—Active mode. • passive—Passive mode. • client—Client mode. • server—Server mode. • bdcast—Broadcast server mode. • control—Control query mode. • private—Private message mode.
local poll	Poll interval of the local device, in seconds. The value displayed is a power of 2. For example, if the displayed value is 6, the poll interval of the local device is 26, or 64 seconds.
peer mode	<p>Operation mode of the peer device:</p> <ul style="list-style-type: none"> • unspec—The mode is unspecified. • active—Active mode. • passive—Passive mode. • client—Client mode. • server—Server mode. • bdcast—Broadcast server mode. • control—Control query mode. • private—Private message mode.
peer poll	Poll interval of the peer device, in seconds. The value displayed is a power of 2. For example, if the displayed value is 6, the poll interval of the local device is 26, or 64 seconds.
offset	Offset of the system clock relative to the reference clock, in milliseconds.
delay	Roundtrip delay from the local device to the clock source, in milliseconds.
disper	Maximum error of the system clock relative to the reference clock.
root delay	Roundtrip delay from the local device to the primary reference source, in milliseconds.
root disper	Maximum error of the system clock relative to the primary reference clock, in milliseconds.
reach	Reachability count of the clock source. A value of 0 indicates that the clock source is unreachable.
sync dist	Synchronization distance relative to the upper-level clock, in seconds, and calculated from dispersion and roundtrip delay values.
sync state	<p>State of the state machine.</p> <p>Displayed value is an integer in the range of 0 to 5.</p>
precision	Precision of the system clock.
version	<p>NTP version.</p> <p>Displayed value is an integer in the range of 1 to 4.</p>

Field	Description
peer interface	Source interface. If the source interface is not specified, this field is wildcard .
reftime	Reference timestamp in the NTP message.
orgtime	Originate timestamp in the NTP message.
rcvtime	Receive timestamp in the NTP message.
xmtime	Transmit timestamp in the NTP message.
filter delay	Delay information.
filter offset	Offset information.
filter disper	Dispersion information.
Total associations	Total number of associations.

When a device is operating in NTP broadcast/multicast server mode, executing the **display ntp-service sessions** command on the device does not display NTP session information corresponding to the broadcast/multicast server, but the sessions are counted in the total number of associations.

display ntp-service status

Syntax

display ntp-service 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 ntp-service status** to display the NTP service status.

Examples

Display the NTP service status.

```
<Sysname> display ntp-service status
Clock status: unsynchronized
Clock stratum: 16
Reference clock ID: none
Nominal frequency: 100.0000 Hz
```

```

Actual frequency: 100.0000 Hz
Clock precision: 2^17
Clock offset: 0.0000 ms
Root delay: 0.00 ms
Root dispersion: 0.00 ms
Peer dispersion: 0.00 ms
Reference time: 00:00:00.000 UTC Jan 1 1900(00000000.00000000)

```

Table 5 Command output

Field	Description
Clock status	Status of the system clock: <ul style="list-style-type: none"> • Synchronized—The system clock has been synchronized. • Unsynchronized—The system clock has not been synchronized.
Clock stratum	Stratum level of the system clock.
Reference clock ID	When the system clock is synchronized to a remote time server, this field indicates the address of the remote time server. When the system clock is synchronized to a local reference source, this field indicates the address of the local clock source: <ul style="list-style-type: none"> • When the local clock has a stratum level of 1, the value of this field is LOCL. • When the stratum of the local clock has another value, the value of this field is the IP address of the local clock.
Nominal frequency	Nominal frequency of the local system hardware clock, in Hz.
Actual frequency	Actual frequency of the local system hardware clock, in Hz.
Clock precision	Precision of the system clock.
Clock offset	Offset of the system clock relative to the reference source, in milliseconds.
Root delay	Roundtrip delay from the local device to the primary reference source, in milliseconds.
Root dispersion	Maximum error of the system clock relative to the primary reference source, in milliseconds.
Peer dispersion	Maximum error of the system clock relative to the reference source, in milliseconds.
Reference time	Reference timestamp.

display ntp-service trace

Syntax

```
display ntp-service trace [ | { 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 ntp-service trace** to display brief information about each NTP server from the local device back to the primary reference source.

The **display ntp-service trace** command takes effect only when the local device and all the devices on the NTP server chain can reach one another. Otherwise, this command is unable to display all the NTP servers on the NTP chain due to timeout.

Examples

Display brief information about each NTP server from the local device back to the primary reference source.

```
<Sysname> display ntp-service trace
server 127.0.0.1, stratum 2, offset -0.013500, synch distance 0.03154
server 133.1.1.1, stratum 1, offset -0.506500, synch distance 0.03429
refid LOCL
```

The output shows an NTP server chain for server 127.0.0.1: Server 127.0.0.1 is synchronized to server 133.1.1.1, and server 133.1.1.1 is synchronized to the local clock source.

Table 6 Command output

Field	Description
server	IP address of the NTP server.
stratum	Stratum level of the corresponding system clock.
offset	Clock offset relative to the upper-level clock, in seconds.
synch distance	Synchronization distance relative to the upper-level clock, in seconds, and calculated from dispersion and roundtrip delay values.
refid	Identifier of the primary reference source. When the stratum level of the primary reference clock is 0, it is displayed as LOCL . Otherwise, it is displayed as the IP address of the primary reference clock.

ntp-service access

Syntax

ntp-service access { peer | query | server | synchronization } acl-number

undo ntp-service access { peer | query | server | synchronization }

View

System view

Default level

3: Manage level

Parameters

peer: Permits full access. This level of right permits the peer devices to perform synchronization and control query to the local device and also permits the local device to synchronize its clock to that of a peer device. Control query refers to query of NTP status information, such as alarm information, authentication status, and clock source information.

query: Permits control query. This level of right permits the peer devices to perform control query to the NTP service on the local device but does not permit a peer device to synchronize its clock to that of the local device.

server: Permits server access and query. This level of right permits the peer devices to perform synchronization and control query to the local device but does not permit the local device to synchronize its clock to that of a peer device.

synchronization: Permits server access only. This level of right permits a peer device to synchronize its clock to that of the local device but does not permit the peer devices to perform control query.

acl-number: Specifies a basic ACL number in the range of 2000 to 2999.

Description

Use **ntp-service access** to configure the access-control right for the peer devices to access the NTP services of the local device.

Use **undo ntp-service access** to remove the configured NTP service access-control right to the local device.

By default, the access-control right for the peer devices to access the NTP services of the local device is set to **peer**.

From the highest NTP service access-control right to the lowest one are **peer**, **server**, **synchronization**, and **query**. When a device receives an NTP request, it matches against the access-control right in this order and uses the first matched right. If no matched right is found, the device drops the NTP request.

The **ntp-service access** command provides only a minimum degree of security protection. A more secure method is identity authentication. The related command is **ntp-service authentication enable**.

Before specifying an ACL number in the **ntp-service access** command, make sure you have already created and configured this ACL.

Examples

```
# Configure the peer devices on subnet 10.10.0.0/16 to have the full access right to the local device.
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-basic-2001] quit
[Sysname] ntp-service access peer 2001
```

ntp-service authentication enable

Syntax

ntp-service authentication enable

undo ntp-service authentication enable

View

System view

Default level

3: Manage level

Parameters

None

Description

Use **ntp-service authentication enable** to enable NTP authentication.

Use **undo ntp-service authentication enable** to disable NTP authentication.

By default, NTP authentication is disabled.

Related commands: **ntp-service authentication-keyid** and **ntp-service reliable authentication-keyid**.

Examples

```
# Enable NTP authentication.  
<Sysname> system-view  
[Sysname] ntp-service authentication enable
```

ntp-service authentication-keyid

Syntax

```
ntp-service authentication-keyid keyid authentication-mode md5 [ cipher | simple ] value  
undo ntp-service authentication-keyid keyid
```

View

System view

Default level

3: Manage level

Parameters

keyid: Specifies an authentication key ID in the range of 1 to 4294967295.

cipher: Sets a ciphertext key.

simple: Sets a plaintext key. This key will be saved in cipher text for security purposes.

value: Specifies the MD5 authentication key string. This argument is case sensitive. If **simple** is specified, it is a string of 1 to 32 characters. If **cipher** is specified, it is a string of 1 to 73 characters. If neither **cipher** nor **simple** is specified, you set a plaintext key string.

Description

Use **ntp-service authentication-keyid** to set the NTP authentication key.

Use **undo ntp-service authentication-keyid** to remove the set NTP authentication key.

By default, no NTP authentication key is set.

In a network where there is a high security demand, the NTP authentication feature should be enabled for a system running NTP. This feature enhances the network security by means of the client-server key authentication, which prohibits a client from synchronizing with a device that has failed authentication.

When the NTP authentication key is configured, configure the key as a trusted key by using the **ntp-service reliable authentication-keyid** command.

Presently the system supports only the MD5 algorithm for key authentication.

A maximum of 1,024 keys can be set for each device.

If an NTP authentication key is specified as a trusted key, the key automatically changes to untrusted after you delete the key. In this case, you do not need to execute the **undo ntp-service reliable authentication-keyid** command.

Related commands: **ntp-service reliable authentication-keyid**.

Examples

Set an MD5 authentication key, with the key ID of 10 and key value of **BetterKey**.

```
<Sysname> system-view
[Sysname] ntp-service authentication enable
[Sysname] ntp-service authentication-keyid 10 authentication-mode md5 BetterKey
```

ntp-service broadcast-client

Syntax

ntp-service broadcast-client

undo ntp-service broadcast-client

View

Interface view

Default level

3: Manage level

Parameters

None

Description

Use **ntp-service broadcast-client** to configure the device to operate in NTP broadcast client mode and use the current interface to receive NTP broadcast packets.

Use **undo ntp-service broadcast-client** to remove the configuration.

By default, the device does not operate in any NTP operation mode.

Examples

Configure the device to operate in broadcast client mode and receive NTP broadcast messages on VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service broadcast-client
```

ntp-service broadcast-server

Syntax

ntp-service broadcast-server [authentication-keyid *keyid* | version *number*] *

undo ntp-service broadcast-server

View

Interface view

Default level

3: Manage level

Parameters

authentication-keyid *keyid*: Specifies the key ID to be used for sending broadcast messages to broadcast clients. The value range for the *keyid* argument is 1 to 4294967295. This parameter is not meaningful if authentication is not required.

version *number*: Specifies the NTP version. The value range for the *number* argument is 1 to 4, and the default is 3.

Description

Use **ntp-service broadcast-server** to configure the device to operate in NTP broadcast server mode and use the current interface to send NTP broadcast packets.

Use **undo ntp-service broadcast-server** to remove the configuration.

By default, the device does not operate in any NTP operation mode.

Examples

Configure the device to operate in broadcast server mode and send NTP broadcast messages on VLAN-interface 1, using key 4 for encryption, and set the NTP version to 3.

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

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

```
[Sysname-Vlan-interface1] ntp-service broadcast-server authentication-keyid 4 version 3
```

ntp-service dscp

Syntax

ntp-service dscp *dscp-value*

undo ntp-service dscp

View

System view

Default level

2: System level

Parameters

dscp-value: Specifies the Differentiated Services Code Point (DSCP) value for NTP messages, in the range of 0 to 63.

Description

Use the **ntp-service dscp** command to set the DSCP value for NTP messages.

Use the **undo ntp-service dscp** command to restore the default.

By default, the DSCP value for NTP messages is 16.

Examples

```
# Set the DSCP value to 30 for NTP messages.
<Sysname> system-view
[Sysname] ntp-service dscp 30
```

ntp-service in-interface disable

Syntax

```
ntp-service in-interface disable
undo ntp-service in-interface disable
```

View

Interface view

Default level

3: Manage level

Parameters

None

Description

Use **ntp-service in-interface disable** to disable an interface from receiving NTP messages.

Use **undo ntp-service in-interface disable** to restore the default.

By default, all interfaces are enabled to receive NTP messages.

Examples

```
# Disable VLAN-interface 1 from receiving NTP messages.
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service in-interface disable
```

ntp-service max-dynamic-sessions

Syntax

```
ntp-service max-dynamic-sessions number
undo ntp-service max-dynamic-sessions
```

View

System view

Default level

3: Manage level

Parameters

number: Sets the maximum number of dynamic NTP sessions that are allowed to be established, in the range of 0 to 100.

Description

Use **ntp-service max-dynamic-sessions** to set the maximum number of dynamic NTP sessions that are allowed to be established locally.

Use **undo ntp-service max-dynamic-sessions** to restore the maximum number of dynamic NTP sessions to the system default.

By default, the number is 100.

A single device can have a maximum of 128 concurrent associations, including static associations and dynamic associations. A static association refers to an association that a user has manually created by using an NTP command, while a dynamic association is a temporary association created by the system during operation. A dynamic association is removed if the system fails to receive messages from it over a specific long period of time. In client/server mode, for example, when you carry out a command to synchronize the time to a server, the system creates a static association, and the server just responds passively upon the receipt of a message, rather than creating an association (static or dynamic). In symmetric mode, static associations are created at the symmetric-active peer side, and dynamic associations are created at the symmetric-passive peer side. In broadcast or multicast mode, static associations are created at the server side, and dynamic associations are created at the client side.

Examples

```
# Set the maximum number of dynamic NTP sessions allowed to be established to 50.
<Sysname> system-view
[Sysname] ntp-service max-dynamic-sessions 50
```

ntp-service multicast-client

Syntax

```
ntp-service multicast-client [ ip-address ]
undo ntp-service multicast-client [ ip-address ]
```

View

Interface view

Default level

3: Manage level

Parameters

ip-address: Sets a multicast IP address. The default is 224.0.1.1.

Description

Use **ntp-service multicast-client** to configure the device to operate in NTP multicast client mode and use the current interface to receive NTP multicast packets.

Use **undo ntp-service multicast-client** to remove the configuration.

By default, the device does not operate in any NTP operation mode.

Examples

```
# Configure the device to operate in multicast client mode and receive NTP multicast messages on
VLAN-interface 1, and set the multicast address to 224.0.1.1.
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service multicast-client 224.0.1.1
```

ntp-service multicast-server

Syntax

```
ntp-service multicast-server [ ip-address ] [ authentication-keyid keyid | ttl ttl-number | version number ]  
*
```

```
undo ntp-service multicast-server [ ip-address ]
```

View

Interface view

Default level

3: Manage level

Parameters

ip-address: Sets a multicast IP address. The default is 224.0.1.1.

authentication-keyid *keyid*: Specifies the key ID to be used for sending multicast messages to multicast clients, where *keyid* is in the range of 1 to 4294967295. This parameter is not meaningful if authentication is not required.

tth *ttl-number*: Specifies the TTL of NTP multicast messages. The value range for the *ttl-number* argument is 1 to 255, and the default is 16.

version *number*: Specifies the NTP version. The value range for the *number* argument is 1 to 4, and the default is 3.

Description

Use **ntp-service multicast-server** to configure the device to operate in NTP multicast server mode and use the current interface to send NTP multicast packets.

Use **undo ntp-service multicast-server** to remove the configuration.

By default, the device does not operate in any NTP operation mode.

Examples

```
# Configure the device to operate in multicast server mode and send NTP multicast messages on  
VLAN-interface 1 to the multicast address 224.0.1.1, using key 4 for encryption, and set the NTP version  
to 3.
```

```
<Sysname> system-view  
[Sysname] interface vlan-interface 1  
[Sysname-Vlan-interface1] ntp-service multicast-server 224.0.1.1 version 3  
authentication-keyid 4
```

ntp-service reliable authentication-keyid

Syntax

```
ntp-service reliable authentication-keyid keyid
```

```
undo ntp-service reliable authentication-keyid keyid
```

View

System view

Default level

3: Manage level

Parameters

keyid: Specifies an authentication key number in the range of 1 to 4294967295.

Description

Use **ntp-service reliable authentication-keyid** to specify that the created authentication key is a trusted key. When NTP authentication is enabled, a client can be synchronized only to a server that can provide a trusted authentication key.

Use **undo ntp-service reliable authentication-keyid** to remove the configuration.

By default, no authentication key is configured to be trusted.

Examples

Enable NTP authentication, specify the use of MD5 encryption algorithm, with the key ID of 37 and key value of **BetterKey**.

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

```
[Sysname] ntp-service authentication enable
```

```
[Sysname] ntp-service authentication-keyid 37 authentication-mode md5 BetterKey
```

Specify this key as a trusted key.

```
[Sysname] ntp-service reliable authentication-keyid 37
```

ntp-service source-interface

Syntax

ntp-service source-interface *interface-type interface-number*

undo ntp-service source-interface

View

System view

Default level

3: Manage level

Parameters

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

Description

Use **ntp-service source-interface** to specify the source interface for NTP messages.

Use **undo ntp-service source-interface** to restore the default.

By default, no source interface is specified for NTP messages, and the system uses the IP address of the interface determined by the matched route as the source IP address of NTP messages.

If you do not want the IP address of a certain interface on the local device to become the destination address of response messages, use this command to specify the source interface for NTP messages so that the source IP address in NTP messages is the primary IP address of this interface.

If the specified source interface goes down, NTP searches the routing table for the outgoing interface, and uses the primary IP address of the outgoing interface as the source IP address.

Examples

```
# Specify the source interface of NTP messages as VLAN-interface 1.
<Sysname> system-view
[Sysname] ntp-service source-interface vlan-interface 1
```

ntp-service unicast-peer

Syntax

```
ntp-service unicast-peer { ip-address | peer-name } [ authentication-keyid keyid | priority | source-interface interface-type interface-number | version number ] *
undo ntp-service unicast-peer { ip-address | peer-name }
```

View

System view

Default level

3: Manage level

Parameters

peer-name: Specifies a host name of the symmetric-passive peer, a string of 1 to 20 characters.

authentication-keyid *keyid*: Specifies the key ID to be used for sending NTP messages to the peer, where *keyid* is in the range of 1 to 4294967295.

priority: Specifies the peer designated by *ip-address* or *peer-name* as the first choice under the same condition.

source-interface *interface-type interface-number*: Specifies the source interface for NTP messages. In an NTP message that the local device sends to its peer, the source IP address is the primary IP address of this interface.

version *number*: Specifies the NTP version. The value range for the *number* argument is 1 to 4, and the default is 3.

Description

Use **ntp-service unicast-peer** to designate a symmetric-passive peer for the device.

Use **undo ntp-service unicast-peer** to remove the symmetric-passive peer designated for the device.

By default, no symmetric-passive peer is designated for the device.

Examples

```
# Designate the device with the IP address of 10.1.1.1 as the symmetric-passive peer of the device,
configure the device to run NTP version 3, and specify the source interface of NTP messages as
VLAN-interface 1.
```

```
<Sysname> system-view
[Sysname] ntp-service unicast-peer 10.1.1.1 version 3 source-interface vlan-interface 1
```

ntp-service unicast-server

Syntax

```
ntp-service unicast-server { ip-address | server-name } [ authentication-keyid keyid | priority | source-interface interface-type interface-number | version number ] *
```

undo ntp-service unicast-server { *ip-address* | *server-name* }

View

System view

Default level

3: Manage level

Parameters

server-name: Specifies a host name of the NTP server, a string of 1 to 20 characters.

authentication-keyid *keyid*: Specifies the key ID to be used for sending NTP messages to the NTP server, where *keyid* is in the range of 1 to 4294967295.

priority: Specifies this NTP server as the first choice under the same condition.

source-interface *interface-type interface-number*: Specifies the source interface for NTP messages. In an NTP message that the local device sends to the NTP server, the source IP address is the primary IP address of this interface.

version *number*: Specifies the NTP version. The value range for the *number* argument is 1 to 4, and the default is 3.

Description

Use **ntp-service unicast-server** to designate an NTP server for the device.

Use **undo ntp-service unicast-server** to remove an NTP server designated for the device.

By default, no NTP server is designated for the device.

Examples

Designate NTP server 10.1.1.1 for the device, and configure the device to run NTP version 3.

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

```
[Sysname] ntp-service unicast-server 10.1.1.1 version 3
```

Information center configuration commands

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

display channel

Syntax

display channel [*channel-number* | *channel-name*] [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

channel-number: Specifies a channel by its number in the range of 0 to 9.

channel-name: Specifies a channel by its name, a default name or a self-defined name. For information about configuring a channel name, see **info-center channel name**.

Table 7 Information channels for different output destinations

Output destination	Information channel number	Default channel name
Console	0	console
Monitor terminal	1	monitor
Log host	2	loghost
Trap buffer	3	trapbuffer
Log buffer	4	logbuffer
SNMP module	5	snmpagent
Web interface	6	channel6

|: 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 channel** to display channel information.

If no channel is specified, the command displays information about all channels.

Examples

Display information about channel 0.

```
<Sysname> display channel 0
channel number:0, channel name:console
MODU_ID  NAME      ENABLE LOG_LEVEL      ENABLE TRAP_LEVEL      ENABLE DEBUG_LEVEL
ffff0000 default  Y      informational      Y      debugging      Y      debugging
```

The output shows that the system is allowed to output log information with a severity from 0 to 4, trap information with a severity from 0 to 7, and debug information with a severity from 0 to 7 to the console. The information source modules are all modules (default).

Table 8 Command output

Field	Description
channel number	Channel number, in the range of 0 to 9.
channel name	Channel name. For more information, see info-center channel name .
MODU_ID	ID of the source module.
NAME	Name of the source module. default means all modules are allowed to output system information, but the actual permitted modules depends on the switch model.
ENABLE	Indicates whether log output is enabled: Y or N.
LOG_LEVEL	Log information severity. See Table 9 for details.
ENABLE	Indicates whether trap output is enabled: Y or N.
TRAP_LEVEL	Trap information severity. See Table 9 for details.
ENABLE	Indicates whether debug output is enabled: Y or N.
DEBUG_LEVEL	Debug information severity. See Table 9 for details.

display info-center

Syntax

```
display info-center [ | { 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 info-center** to display information center configuration information.

Examples

```
# Display information center configuration information.
<Sysname> display info-center
Information Center:enabled
Log host:
    1.1.1.1,
    port number : 514, host facility : local7,
    channel number : 2, channel name : loghost
Console:
    channel number : 0, channel name : console
Monitor:
    channel number : 1, channel name : monitor
SNMP Agent:
    channel number : 5, channel name : snmpagent
Log buffer:
    enabled,max buffer size 1024, current buffer size 512,
    current messages 512, dropped messages 0, overwritten messages 740
    channel number : 4, channel name : logbuffer
Trap buffer:
    enabled,max buffer size 1024, current buffer size 256,
    current messages 216, dropped messages 0, overwritten messages 0
    channel number : 3, channel name : trapbuffer
syslog:
    channel number:6, channel name:channel6
Information timestamp setting:
    log - date, trap - date, debug - date,
    loghost - date
```

display logbuffer

Syntax

```
display logbuffer [ reverse ] [ level severity | size buffersize | slot slot-number ] * [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

reverse: Displays log entries chronologically, with the most recent entry at the top. Without this keyword, the command displays log entries chronologically, with the oldest entry at the top.

level *severity*: Specifies a severity level in the range of 0 to 7.

Table 9 Severity description

Severity	Value	Description	Corresponding keyword in commands
Emergency	0	The system is unusable.	emergencies
Alert	1	Action must be taken immediately.	alerts
Critical	2	Critical condition.	critical
Error	3	Error condition.	errors
Warning	4	Warning condition.	warnings
Notification	5	Normal but significant condition.	notifications
Informational	6	Informational message.	informational
Debug	7	Debugging message.	debugging

size *buffersize*: Specifies the number of latest log messages to be displayed, in the range of 1 to 1024.

slot *slot-number*: Specifies an IRF member ID.

|: 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 logbuffer** to display the state of the log buffer and the log information in the log buffer. Without **size** *buffersize*, the command displays all log information in the log buffer.

Examples

Display the state and log information about the log buffer.

```
<Sysname> display logbuffer
Logging buffer configuration and contents:enabled
Allowed max buffer size : 1024
Actual buffer size : 512
Channel number : 4 , Channel name : logbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 127
```

```
%Jun 19 18:03:24:55 2011 Sysname IC/7/SYS_RESTART:
System restarted --
...
```

Table 10 Command output

Field	Description
Logging buffer configuration and contents	State of the log buffer: enabled or disabled.

Field	Description
Allowed max buffer size	Maximum number of messages that can be stored in the log buffer.
Actual buffer size	Actual buffer size.
Channel number	Channel number of the log buffer. The default channel number is 4.
Channel name	Channel name of the log buffer. The default channel name is logbuffer.
Dropped messages	Number of dropped messages.
Overwritten messages	Number of overwritten messages (when the buffer size is not big enough to hold all messages, the latest messages overwrite the old ones).
Current messages	Number of current messages.

display logbuffer summary

Syntax

display logbuffer summary [**level** *severity* | **slot** *slot-number*] * [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

level *severity*: Specifies a severity level in the range of 0 to 7.

slot *slot-number*: Specifies an IRF member ID.

|: 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 logbuffer summary** to display the summary of the log buffer.

Examples

Display the summary of the log buffer.

```
<Sysname> display logbuffer summary
  SLOT EMERG ALERT  CRIT ERROR  WARN NOTIF  INFO DEBUG
    1      0      0      0      0      0      0      0      0
    2      0      0      0      0      0      0      0      0
```


3 0 0 0 0 16 0 1 0

Table 11 Command output

Field	Description
SLOT	ID of an IRF member switch
EMERG	Represents emergency, see Table 9 for details
ALERT	Represents alert, see Table 9 for details
CRIT	Represents critical, see Table 9 for details
ERROR	Represents error, see Table 9 for details
WARN	Represents warning, see Table 9 for details
NOTIF	Represents notice, see Table 9 for details
INFO	Represents informational, see Table 9 for details
DEBUG	Represents debug, see Table 9 for details

display security-logfile buffer

Syntax

display security-logfile buffer [| { **begin** | **exclude** | **include** } *regular-expression*]

View

User 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 security-logfile buffer** to display the contents of the security log file buffer.

The system buffers security logs into the security log file buffer temporarily. When a saving operation is performed automatically or manually, the system saves the contents of the security log file buffer into the security log file, and then clears the security log file buffer.

A local user can use this command only after being authorized as the security log administrator by the system administrator through the **authorization-attribute user-role security-audit** command. For details of the **authorization-attribute** command, see *Security Command Reference*.

Related commands: **info-center security-logfile frequency** and **security-logfile save**.

Examples

```
# Display the contents of the security log file buffer.
<Sysname> display security-logfile buffer
%01 Sep 17 11:13:16:609 2011 Sysname SHELL/5/SHELL_LOGIN: Console logged in from aux0.
...
```

display security-logfile summary

Syntax

```
display security-logfile summary [ | { begin | exclude | include } regular-expression ]
```

View

Security log management 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 security-logfile summary** to display the summary of the security log file.

A local user can use this command only after being authorized as the security log administrator by the system administrator through the **authorization-attribute user-role security-audit** command. For more information about the **authorization-attribute** command, see *Security Command Reference*.

Examples

```
# Display the summary of the security log file.
<Sysname> display security-logfile summary
Security log file is enabled
Security log file size quota: 6MB
Security log file directory: flash:/seclog
Alarm-threshold: 80%
Current usage: 30%
Writing frequency: 1 hour 0 min 0 sec
```

Table 12 Command output

Field	Description
Security log file is	State of the security log file feature: enabled or disabled.
Security log file size quota	Maximum size of the security log file.
Security log file directory	Security log file directory.

Field	Description
Alarm-threshold	Alarm threshold of the security log file usage.
Current usage	Current usage of the security log file.
Writing frequency	Interval at which the system saves security logs from the security log file buffer to the security log file.

display trapbuffer

Syntax

display trapbuffer [**reverse**] [**size** *buffersize*] [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

reverse: Displays trap entries chronologically, with the most recent entry at the top. Without this keyword, the command displays trap entries chronologically, with the oldest entry at the top.

size *buffersize*: Specifies the number of latest trap messages to be displayed, in the range of 1 to 1024.

|: 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 trapbuffer** to display the state and the trap information of the trap buffer. Without the **size buffersize** argument, the command displays all trap information.

Examples

Display the state and trap information of the trap buffer. (The actual command output depends on the operations executed on the switch.)

```
<Sysname> display trapbuffer
Trapping buffer configuration and contents:enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 9

#Jan  7 08:03:27:421 2011 Sysname IFNET/4/INTERFACE UPDOWN:
```

Trap 1.3.6.1.6.3.1.1.5.4<linkUp>: Interface 983041 is Up, ifAdminStatus is 1, ifOperStatus is 1

Table 13 Command output

Field	Description
Trapping buffer configuration and contents	State of the trap buffer: enabled or disabled.
Allowed max buffer size	Maximum capacity of the trap buffer.
Actual buffer size	Actual capacity of the trap buffer.
Channel number	Channel number of the trap buffer, which defaults to 3.
channel name	Channel name of the trap buffer, which defaults to trapbuffer.
Dropped messages	Number of dropped messages.
Overwritten messages	Number of overwritten messages (when the buffer size is not big enough to hold all messages, the latest messages overwrite the old ones).
Current messages	Number of current messages.

enable log updown

Syntax

enable log updown

undo enable log updown

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **enable log updown** to enable an interface to generate link up or link down logging information when the interface state changes.

Use **undo enable log updown** to disable an interface from generating link up or link down logging information when the interface state changes.

By default, all the interfaces are allowed to generate link up or link down logging information when the interface state changes.

Examples

Disable port GigabitEthernet1/0/1 from generating link up or link down logging information.

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

```
[Sysname] interface GigabitEthernet1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] undo enable log updown
```

info-center channel name

Syntax

info-center channel *channel-number* **name** *channel-name*

undo info-center channel *channel-number*

View

System view

Default level

2: System level

Parameters

channel-number: Specifies a channel by its number in the range of 0 to 9.

channel-name: Specifies a channel name, a case-insensitive string of 1 to 30 characters. It must be a combination of letters and numbers and start with a letter.

Description

Use **info-center channel name** to name a channel.

Use **undo info-center channel** to restore the default name for a channel.

See [Table 7](#) for information about default channel names and channel numbers.

Examples

Name channel 0 **abc**.

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

```
[Sysname] info-center channel 0 name abc
```

info-center console channel

Syntax

info-center console channel { *channel-number* | *channel-name* }

undo info-center console channel

View

System view

Default level

2: System level

Parameters

channel-number: Specifies a channel by its number in the range of 0 to 9.

channel-name: Specifies a channel by its name, a default name or a self-defined name. For information about configuring a channel name, see **info-center channel name**.

Description

Use **info-center console channel** to specify the console output channel. The system uses this channel to output information to the console.

Use **undo info-center console channel** to restore the default console output channel.

The default console output channel is channel 0.

The **info-center console channel** command takes effect only when the information center has been enabled with the **info-center enable** command.

Examples

Specify the console output channel as channel 0.

```
<Sysname> system-view
[Sysname] info-center console channel 0
```

info-center enable

Syntax

info-center enable

undo info-center enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **info-center enable** to enable the information center.

Use **undo info-center enable** to disable the information center.

The switch can output system information only after the information center is enabled.

By default, the information center is enabled.

Examples

Enable the information center.

```
<Sysname> system-view
[Sysname] info-center enable
Info: Information center is enabled.
```

info-center format unicom

Syntax

info-center format unicom

undo info-center format

View

System view

Default level

2: System level

Parameters

None

Description

Use **info-center format unicom** to set the UNICOM format for system information sent to a log host.

Use **undo info-center format** to restore the default.

By default, system information is sent to a log host in HP format.

System information can be sent to a log host in HP or UNICOM format. For more information, see *Network Management and Monitoring Configuration Guide*.

Examples

```
# Set the UNICOM format for system information sent to a log host.
```

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

```
[Sysname] info-center format unicom
```

info-center logbuffer

Syntax

info-center logbuffer [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*] *

undo info-center logbuffer [**channel** | **size**]

View

System view

Default level

2: System level

Parameters

channel-number: Specifies a channel by its number in the range of 0 to 9.

channel-name: Specifies a channel by its name, a default name or a self-defined name. For information about configuring a channel name, see **info-center channel name**.

buffersize: Specifies the maximum number of log messages that can be stored in the log buffer, in the range of 0 to 1024.

Description

Use **info-center logbuffer** to configure information output to the log buffer.

Use **undo info-center logbuffer** to disable information output to the log buffer.

By default, the system outputs information to the log buffer through channel 4 (logbuffer), and the default buffer size is 512.

The **info-center logbuffer** command takes effect only when the information center has been enabled with the **info-center enable** command.

Examples

```
# Output system information to the log buffer through channel 4, and set the log buffer size to 50.
```

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

```
[Sysname] info-center logbuffer size 50
```

info-center logfile overwrite-protection

Syntax

info-center logfile overwrite-protection [**all-port-powerdown**]

undo info-center logfile overwrite-protection

View

System view

Default level

2: System level

Parameters

all-port-powerdown: Shuts down all the physical ports on the device except for the console port and physical ports that have been bound to an IRF port when the capacity of the log file reaches the upper limit or the storage device runs out of flash. To restore the device to the normal state, first back up the log file and delete the original file, and then bring up the interfaces.

Description

Use **info-center logfile overwrite-protection** to enable the log file overwrite-protection function. When the capacity of the log file reaches the upper limit or the storage device runs out of memory, new logs cannot be written into the log file.

Use **undo info-center logfile overwrite-protection** to disable the log file overwrite-protection function. When the capacity of the log file reaches the upper limit or the storage device runs out of flash, the device deletes the oldest logs in the log file and writes new logs into the log file.

This command is available only in FIPS mode.

By default, log file overwrite-protection is disabled.

Examples

```
# Enable the log file overwrite-protection function.
<Sysname> system-view
[Sysname] info-center logfile overwrite-protection
```

info-center loghost

Syntax

info-center loghost { *host-ipv4-address* | **ipv6** *host-ipv6-address* } [**port** *port-number*] [**dscp** *dscp-value*] [**channel** { *channel-number* | *channel-name* } | **facility** *local-number*] *

undo info-center loghost { *host-ipv4-address* | **ipv6** *host-ipv6-address* }

View

System view

Default level

2: System level

Parameters

ipv6 *host-ipv6-address*: Specifies the IPv6 address of a log host.

host-ipv4-address: Specifies the IPv4 address of a log host.

port *port-number*: Specifies the port number of the log host, in the range of 1 to 65535. The default value is 514. It must be the same as the value configured on the log host. Otherwise, the log host cannot receive system information.

dscp *dscp-value*: Specifies the DSCP value for the packets sent to the log host. The value range is 0 to 63, and the default is 0.

channel: Specifies the channel through which system information is output to the log host.

channel-number: Specifies a channel number in the range of 0 to 9.

channel-name: Specifies a channel name, a default name or a self-defined name. For information about configuring a channel name, see the **info-center channel name** command.

facility *local-number*: Specifies a logging facility from local0 to local7 for the log host. The default value is local7. Logging facilities are used to mark different logging sources, and query and filter logs.

Description

Use **info-center loghost** to specify a log host and configure output parameters.

Use **undo info-center loghost** to restore the default.

By default, no log host is specified.

If you configure this command without specifying a channel, the system specifies channel 2 (loghost) by default.

The **info-center loghost** command takes effect only when the information center has been enabled with the **info-center enable** command.

Enter a correct log host IP address. The system prompts an invalid address if you enter an incorrect IP address, such as an IPv6 loopback address or a broadcast address.

The switch supports up to four log hosts.

Examples

Output log information to the IPv4 log host 1.1.1.1.

```
<Sysname> system-view
[Sysname] info-center loghost 1.1.1.1
```

Output log information to the IPv6 log host 1::1.

```
<Sysname> system-view
[Sysname] info-center loghost ipv6 1::1
```

info-center loghost source

Syntax

info-center loghost source *interface-type interface-number*

undo info-center loghost source

View

System view

Default level

2: System level

Parameters

interface-type interface-number: Specifies the egress interface for log information by the interface type and interface number.

Description

Use **info-center loghost source** to specify the source IP address for output log information.

Use **undo info-center loghost source** to restore the default.

By default, the source IP address of output log information is the primary IP address of the matching route's egress interface.

The system uses the primary IP address of the specified egress interface as the source IP address of log information no matter which physical interface is used to output the log information. If you want to display the source IP address in the log information, you can configure it by using this command.

The **info-center loghost source** command takes effect only after the information center is enabled with the **info-center enable** command.

The IP address of the specified egress interface must have been configured. Otherwise, although the **info-center loghost source** command can be configured successfully, the log host cannot receive any log information.

Examples

When no source IP address is specified for log information, log in to the FTP server using the username **ftp**. The following log information is displayed on the log host:

```
<189>Jan 31 05:37:52 2011 Sysname %%10FTPD/5/FTPD_LOGIN(1): User ftp (192.168.1.23) has logged in successfully.
```

Specify the IP address of the VLAN interface as the source IP address of log information.

```
<Sysname> system-view
[Sysname] vlan 100
[Sysname-vlan100] interface vlan-interface 100
[Sysname-Vlan-interface100] ip address 2.2.2.2 24
[Sysname-Vlan-interface100] quit
[Sysname] info-center loghost source Vlan-interface 100
```

After the above configuration, log in to the FTP server by using the username **ftp**. The following log information is displayed on the log host (the **-DevIP=2.2.2.2** field identifies the source IP address):

```
<189>May 31 05:38:14 2011 Sysname %%10FTPD/5/FTPD_LOGIN(1): -DevIP=2.2.2.2; User ftp (192.168.1.23) has logged in successfully.
```

info-center monitor channel

Syntax

info-center monitor channel { *channel-number* | *channel-name* }

undo info-center monitor channel

View

System view

Default level

2: System level

Parameters

channel-number: Specifies a channel by its number in the range of 0 to 9.

channel-name: Specifies a channel by its name, a default name or a self-defined name. For information about configuring a channel name, see **info-center channel name**.

Description

Use **info-center monitor channel** to configure the monitor channel. The system uses this channel to output information to the monitor.

Use **undo info-center monitor channel** to restore the default monitor output channel.

By default, the system outputs information to the monitor through channel 1 (monitor).

The **info-center monitor channel** command takes effect only after the information center is enabled with the **info-center enable** command.

Examples

```
# Output system information to the monitor through channel 0.
```

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

```
[Sysname] info-center monitor channel 0
```

info-center security-logfile alarm-threshold

Syntax

info-center security-logfile alarm-threshold *usage*

undo info-center security-logfile alarm-threshold

View

System view

Default level

2: System level

Parameters

usage: Specifies an alarm threshold for the security log file. The value must be an integer in the range of 1 to 100.

Description

Use **info-center security-logfile alarm-threshold** to set the alarm threshold of the security log file usage.

Use **undo info-center security-logfile alarm-threshold** to restore the default.

By default, the alarm threshold of the security log file usage is 80. When the usage of the security log file reaches 80%, the system informs the administrator.

When the size of the security log file reaches the upper limit, the system deletes the oldest information and then writes the new information into the security log file buffer. This feature can avoid security log loss by setting an alarm threshold. When the threshold is reached, the system outputs log information to inform the administrator. The administrator can log in to the switch as the security log administrator, and back up the security log file.

Related commands: **info-center security-logfile size-quota**.

Examples

```
# Set the alarm threshold for security log file usage to 90%.
```

```
<Sysname> system-view  
[Sysname] info-center security-logfile alarm-threshold 90
```

info-center security-logfile enable

Syntax

```
info-center security-logfile enable  
undo info-center security-logfile enable
```

View

System view

Default level

2: System level

Parameters

None

Description

Use **info-center security-logfile enable** to enable the saving of the security logs into the security log file.

Use **undo info-center security-logfile enable** to restore the default.

By default, the saving of security logs into the security log file is disabled.

This feature enables the system to put security logs into the security log file buffer, and saves the logs from the buffer to the security log file at a specific interval.

Examples

```
# Enable the saving of the security logs into the security log file.  
<Sysname> system-view  
[Sysname] info-center security-logfile enable
```

info-center security-logfile frequency

Syntax

```
info-center security-logfile frequency freq-sec  
undo info-center security-logfile frequency
```

View

System view

Default level

2: System level

Parameters

freq-sec: Specifies the saving interval in the range of 10 to 86400 seconds.

Description

Use **info-center security-logfile frequency** to configure the interval for saving security logs to the security log file.

Use **undo info-center security-logfile frequency** to restore the default interval.

The default saving interval is 600 seconds.

Related commands: **info-center security-logfile enable**.

Examples

```
# Save security logs to the security log file every 3600 seconds.
```

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

```
[Sysname] info-center security-logfile frequency 3600
```

info-center security-logfile size-quota

Syntax

info-center security-logfile size-quota *size*

undo info-center security-logfile size-quota

View

System view

Default level

2: System level

Parameters

size: Specifies the maximum size of the security log file, in the range of 1 to 10 MB.

Description

Use **info-center security-logfile size-quota** to set the maximum size of the security log file.

Use **undo info-center security-logfile size-quota** to restore the default.

By default, the maximum size of the security log file is 1 MB.

Related commands: **info-center security-logfile alarm-threshold**.

Examples

```
# Set the maximum size of the security log file to 6 MB.
```

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

```
[Sysname] info-center security-logfile size-quota 6
```

info-center security-logfile switch-directory

Syntax

info-center security-logfile switch-directory *dir-name*

View

Any view

Default level

2: System level

Parameters

dir-name: Specifies a directory by its name, a string of 1 to 64 characters.

Description

Use **info-center security-logfile switch-directory** to configure the directory where the security log file is saved.

By default, the security log file is saved in the **seclog** directory under the root directory of the flash.

The specified directory must have been created.

The configuration made by this command cannot survive a system restart or a change of roles of IRF member switches.

A local user can use this command only after being authorized as the security log administrator by the system administrator through the **authorization-attribute user-role security-audit** command. For more information about the **authorization-attribute** command, see *Security Command Reference*.

Examples

```
# Save the security log file to flash:/test.
```

```
<Sysname> mkdir test
```

```
%Created dir flash:/test.
```

```
<Sysname> info-center security-logfile switch-directory flash:/test
```

info-center snmp channel

Syntax

```
info-center snmp channel { channel-number | channel-name }
```

```
undo info-center snmp channel
```

View

System view

Default level

2: System level

Parameters

channel-number: Specifies a channel by its number in the range of 0 to 9.

channel-name: Specifies a channel by its name, a default name or a self-defined name. For information about configuring a channel name, see **info-center channel name**.

Description

Use **info-center snmp channel** to configure the SNMP output channel. The system uses this channel to output information to the SNMP module.

Use **undo info-center snmp channel** to restore the default SNMP output channel.

By default, the system outputs information to the SNMP module through channel 5 (snmpagent).

For more information about SNMP, see "[SNMP configuration commands](#)."

Examples

```
# Output system information to the SNMP module through channel 6.
```

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

```
[Sysname] info-center snmp channel 6
```

info-center source

Syntax

```
info-center source { module-name | default } channel { channel-number | channel-name } [ debug { level severity | state state } * | log { level severity | state state } * | trap { level severity | state state } * ] *  
undo info-center source { module-name | default } channel { channel-number | channel-name }
```

View

System view

Default level

2: System level

Parameters

module-name: Specifies a module. For instance, to output ARP information, specify this argument as ARP. You can use the **info-center source ?** command to view the modules supported by the switch.

default: Specifies all the modules, which can be displayed by using the **info-center source ?** command.

debug: Specifies debug information.

log: Specifies log information.

trap: Specifies trap information.

level severity: Specifies a severity level. See [Table 9](#) for more information.

state state: Specifies whether to output the specified system information, **on** (enabled) or **off** (disabled).

channel-number: Specifies a channel by its number in the range of 0 to 9.

channel-name: Specifies a channel by its name, a default name or a self-defined name. For information about configuring a channel name, see **info-center channel name**.

Description

Use **info-center source** to configure an information output rule for a module.

Use **undo info-center source** to remove the specified output rule.

The default output rules are listed in [Table 14](#).

This command sets an output rule for a specified module or all modules. For example, you can output IP log information with a severity higher than warning to the log host, and output IP log information with a severity higher than informational to the log buffer.

If you do not set an output rule for a module, the module uses the default output rule or the output rule set by using the **default** keyword.

If you use the **default** keyword to set an output rule for all the modules without specifying the **debug**, **log**, and **trap** keywords, the default output rules for the modules are used. See [Table 14](#) for more information.

If you use the *module-name* argument to set the output rule for a module without specifying the **debug**, **log**, and **trap** keywords, the default settings for the module are as follows: the output of log and trap information is enabled, with *severity* being informational; the output of debugging information is disabled, with *severity* being debug. For example, if you execute the command **info-center source cmd channel 0**, the command is actually equal to the command **info-center source cmd 0 debug level debugging state off log level informational state on trap level informational state on**.

If you use the command multiple times, only the most recent output rule takes effect for the specified module.

After you set an output rule for a module, you must use the *module-name* argument to modify or remove the rule. A new output rule configured by using the **default** keyword does not take effect for the module.

The trap buffer only receives trap information and discards log and debug information.

The log buffer only receives log information and discards trap and debug information.

The SNMP module only receives trap information and discards log and debug information.

Table 14 Default output rules

Destination	Source modules	Log		Trap		Debug	
		State	Severity	State	Severity	State	Severity
Console	All supported modules	Enabled	Informational	Enabled	Debug	Enabled	Debug
Monitor terminal	All supported modules	Enabled	Informational	Enabled	Debug	Enabled	Debug
Log host	All supported modules	Enabled	Informational	Enabled	Debug	Disabled	Debug
Trap buffer	All supported modules	Disabled	Informational	Enabled	Informational	Disabled	Debug
Log buffer	All supported modules	Enabled	Informational	Disabled	Debug	Disabled	Debug
SNMP module	All supported modules	Disabled	Debug	Enabled	Informational	Disabled	Debug
Web interface	All supported modules	Enabled	Debug	Enabled	Debug	Disabled	Debug

Examples

Output VLAN module's trap information with a severity level of at least **emergency** to the console channel. All other system information cannot be output to this channel.

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

```
[Sysname] info-center source default channel console debug state off log state off trap state off
```

```
[Sysname] info-center source vlan channel console trap level emergencies state on
```

info-center synchronous

Syntax

info-center synchronous

undo info-center synchronous

View

System view

Default level

2: System level

Parameters

None

Description

Use **info-center synchronous** to enable synchronous information output.

Use **undo info-center synchronous** to disable synchronous information output.

By default, synchronous information output is disabled.

If system information is output before you input information at a command line prompt, the system does not display the command line prompt after the system information output.

If system information is output when you are inputting some interactive information (non Y/N confirmation information), the system displays your input in a new line after the system information output.

Examples

Enable synchronous information output, and then issue the **display current-configuration** command to view the current configuration of the switch.

```
<Sysname> system-view
[Sysname] info-center synchronous
% Info-center synchronous output is on
[Sysname] display current-
```

At this time, the system receives log information. It displays the log information first, and then displays your previous input, which is **display current-** in this example.

```
%Jan 21 14:33:19:425 2011 Sysname SHELL/4/LOGIN: VTY login from 192.168.1.44
[Sysname] display current-
```

Enter **configuration** to complete the **display current-configuration** command, and press **Enter** to execute the command.

Enable synchronous information output, and then save the current configuration (enter interactive information).

```
<Sysname> system-view
[Sysname] info-center synchronous
% Info-center synchronous output is on
[Sysname] save
The current configuration will be written to the device. Are you sure? [Y/N]:
```

At this time, the system receives the log information. It displays the log information first and then displays [Y/N].

```
%Jan 21 14:33:19:425 2011 Sysname SHELL/4/LOGIN: VTY login from 192.168.1.44
[Y/N]:
```

Enter **Y** or **N** to complete your input.

info-center syslog channel

Syntax

info-center syslog channel { *channel-number* | *channel-name* }

undo info-center syslog channel

View

System view

Default level

2: System level

Parameters

channel-number: Specifies a channel by its number in the range of 0 to 9.

channel-name: Specifies a channel by its name, a default name or a self-defined name. For information about configuring a channel name, see **info-center channel name**.

Description

Use **info-center syslog channel** to configure the Web output channel. The system uses this channel to output information to the Web interface.

Use **undo info-center syslog channel** to restore the default.

The default Web output channel is channel 6.

Examples

```
# Output system information to the Web interface through channel 7.  
<Sysname> system-view  
[Sysname] info-center syslog channel 7
```

info-center timestamp

Syntax

info-center timestamp { **debugging** | **log** | **trap** } { **boot** | **date** | **none** }

undo info-center timestamp { **debugging** | **log** | **trap** }

View

System view

Default level

2: System level

Parameters

debugging: Sets the timestamp format for debug information.

log: Sets the timestamp format for log information.

trap: Sets the timestamp format for trap information.

boot: Sets the timestamp format as xxxxxx.yyyyyy, where xxxxxx is the most significant 32 bits (in milliseconds) and yyyyyy is the least significant 32 bits. For example, 0.21990989 equals Jan 25 14:09:26:881 2011. The **boot** time shows the time since system startup.

date: Sets the timestamp format as "Mmm dd hh:mm:ss:sss yyyy". For example, Jan 8 10:12:21:708 2011. The **date** time shows the current system time.

- Mmm: Abbreviations of the months in English, which could be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, or Dec.
- dd: Date, starting with a space if it is less than 10, for example " 7".
- hh:mm:ss:sss: Local time, with hh ranging from 00 to 23, mm and ss ranging from 00 to 59, and sss ranging from 0 to 999.
- yyyy: Year.

none: Indicates that no time information is provided.

Description

Use **info-center timestamp** to configure the timestamp format for system information sent to all destinations except the log host.

Use **undo info-center timestamp** to restore the default.

By default, the timestamp format for system information sent to a log host is set by the **info-center timestamp loghost** command, and the format for log, trap and debug information sent to other destinations is **date**.

Related commands: **info-center timestamp loghost**.

Examples

Configure the timestamp format for log information as **boot**.

```
<Sysname> system-view
[Sysname] info-center timestamp log boot
```

Now, if you log in to the FTP server by using the username **ftp**, the log information generated is as follows:

```
%0.109391473 Sysname FTPD/5/FTPD_LOGIN: User ftp (192.168.1.23) has logged in
successfully.
```

Configure the timestamp format for log information as **date**.

```
<Sysname> system-view
[Sysname] info-center timestamp log date
```

Now, if you log in to the FTP server by using the username **ftp**, the log information generated is as follows:

```
%Jan 30 05:36:29:579 2011 Sysname FTPD/5/FTPD_LOGIN: User ftp (192.168.1.23) has logged
in successfully.
```

Configure the timestamp format for log information as **none**.

```
<Sysname> system-view
[Sysname] info-center timestamp log none
```

Now, if you log in to the FTP server by using the username **ftp**, the log information generated is as follows:

```
% Sysname FTPD/5/FTPD_LOGIN: User ftp (192.168.1.23) has logged in successfully.
```

info-center timestamp loghost

Syntax

info-center timestamp loghost { date | iso | no-year-date | none }

undo info-center timestamp loghost

View

System view

Default level

2: System level

Parameters

date: Sets the timestamp format as "Mmm dd hh:mm:ss yyyy". For example, Jan 8 10:12:21 2011.

iso: Sets the ISO 8601 timestamp format. For example, 2011-01-21T15:32:55.

no-year-date: Sets the timestamp format as the current system date and time without year.

none: Indicates that no timestamp information is provided.

Description

Use **info-center timestamp loghost** to configure the timestamp format for system information sent to the log host.

Use **undo info-center timestamp loghost** to restore the default.

By default, the timestamp format for system information sent to a log host is **date**.

Related commands: **info-center timestamp**.

Examples

Configure the timestamp format for system information sent to a log host as **no-year-date**.

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

```
[Sysname] info-center timestamp loghost no-year-date
```

info-center trapbuffer

Syntax

info-center trapbuffer [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*] *

undo info-center trapbuffer [**channel** | **size**]

View

System view

Default level

2: System level

Parameters

size *buffersize*: Specifies the maximum number of trap messages allowed in the trap buffer, in the range of 0 to 1024. The default value is 256.

channel-number: Specifies a channel by its number in the range of 0 to 9.

channel-name: Specifies a channel by its name, a default name or a self-defined name. For information about configuring a channel name, see **info-center channel name**.

Description

Use **info-center trapbuffer** to enable information output to the trap buffer and set the corresponding parameters.

Use **undo info-center trapbuffer** to disable information output to the trap buffer.

By default, the system outputs information to the trap buffer through channel 3 (trapbuffer), and the maximum buffer size is 256.

The **info-center trapbuffer** command takes effect only after the information center has been enabled with the **info-center enable** command.

Examples

```
# Output system information to the trap buffer through the default channel, and set the trap buffer size to 30.
```

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

```
[Sysname] info-center trapbuffer size 30
```

reset logbuffer

Syntax

reset logbuffer

View

User view

Default level

3: Manage level

Parameters

None

Description

Use **reset logbuffer** to clear the log buffer.

Examples

```
# Clear the log buffer.
```

```
<Sysname> reset logbuffer
```

reset trapbuffer

Syntax

reset trapbuffer

View

User view

Default level

3: Manage level

Parameters

None

Description

Use **reset trapbuffer** to clear the trap buffer.

Examples

```
# Clear the trap buffer.  
<Sysname> reset trapbuffer
```

security-logfile save

Syntax

security-logfile save

View

Any view

Default level

2: System level

Parameters

None

Description

Use **security-logfile save** to manually save security logs from the security log file buffer into the security log file.

By default, the system automatically saves security logs from the security log file buffer into the security log file at the interval configured by the **info-center security-logfile frequency** command. The directory for the security log file can be configured by using the **info-center security-logfile switch-directory** command.

Before backing up the security log file, you can use this command to save the latest security logs in the log buffer into the security log file.

The system clears the security log file buffer after saving security logs into the security log file automatically or manually.

A local user can use this command only after being authorized as the security log administrator by the system administrator through the **authorization-attribute user-role security-audit** command. For more information about the **authorization-attribute** command, see *Security Command Reference*.

Examples

```
# Save the logs in the security log file buffer into the security log file.  
<Sysname> security-logfile save
```

terminal debugging

Syntax

terminal debugging

undo terminal debugging

View

User view

Default level

1: Monitor level

Parameters

None

Description

Use **terminal debugging** to enable the display of debugging information on the current terminal.

Use **undo terminal debugging** to disable the display of debugging information on the current terminal.

By default, the display of debugging information on the current terminal is disabled.

To view debug information, execute the **terminal monitor** and **terminal debugging** commands, enable information center (enabled by default), and finally use a debugging command to enable the related debugging.

The configuration of this command is only valid for the current connection between the terminal and the switch. If a new connection is established, the display of debugging information on the terminal restores the default.

Examples

```
# Enable the display of debugging information on the current terminal.
```

```
<Sysname> terminal debugging
```

```
Info: Current terminal debugging is on.
```

terminal logging

Syntax

terminal logging

undo terminal logging

View

User view

Default level

1: Monitor level

Parameters

None

Description

Use **terminal logging** to enable the display of log information on the current terminal.

Use **undo terminal logging** to disable the display of log information on the current terminal.

By default, the display of log information is enabled on both the current terminal and the console.

To view the log information, execute the **terminal monitor** and **terminal logging** commands, and then enable information center (enabled by default).

The configuration of this command is only valid for the current connection between the terminal and the switch. If a new connection is established, the display of log information on the terminal restores the default.

Examples

```
# Disable the display of log information on the current terminal.
```

```
<Sysname> undo terminal logging
```

Info: Current terminal logging is off.

terminal monitor

Syntax

terminal monitor

undo terminal monitor

View

User view

Default level

1: Monitor level

Parameters

None

Description

Use **terminal monitor** to enable the monitoring of system information on the current terminal.

Use **undo terminal monitor** to disable the monitoring of system information on the current terminal.

By default, monitoring of the system information is enabled on the console and disabled on the current terminal.

Configure the **terminal monitor** command before you can display the log, trap, and debugging information.

The **undo terminal monitor** command automatically disables the monitoring of log, trap, and debugging information.

The configuration of this command is only valid for the current connection between the terminal and the switch. If a new connection is established, the monitoring of system information on the terminal restores the default.

Examples

```
# Enable the monitoring of system information on the current terminal.
```

```
<Sysname> terminal monitor
```

```
Info: Current terminal monitor is on.
```

terminal trapping

Syntax

terminal trapping

undo terminal trapping

View

User view

Default level

1: Monitor level

Parameters

None

Description

Use **terminal trapping** to enable the display of trap information on the current terminal.

Use **undo terminal trapping** to disable the display of trap information on the current terminal.

By default, the display of trap information is enabled on both the current terminal and the console.

To view the trap information, execute the **terminal monitor** and **terminal trapping** commands, and then enable information center (enabled by default).

The configuration of this command is only valid for the current connection between the terminal and the switch. If a new connection is established, the display of trap information on the terminal restores the default.

Examples

Enable the display of trap information on the current terminal.

```
<Sysname> terminal trapping
```

```
Info: Current terminal trapping is on.
```

SNMP configuration commands

display snmp-agent community

Syntax

display snmp-agent community [**read** | **write**] [[{ **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

read: Displays information about SNMP read-only communities.

write: Displays information about SNMP read and write communities.

[: 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 snmp-agent community** to display SNMPv1 and SNMPv2c community information.

This command displays the SNMPv1 and SNMPv2c communities that you have created by using the **snmp-agent community** command or the **snmp-agent usm-user { v1 | v2c }** command.

This command is supported only in non-FIPS mode.

Related commands: **snmp-agent community** and **snmp-agent usm-user { v1 | v2c }**.

Examples

Display information about all SNMPv1 and SNMPv2c communities.

```
<Sysname> display snmp-agent community
Community name: aa
  Group name: aa
  Acl:2001
  Storage-type: nonVolatile

Community name: bb
  Group name: bb
  Storage-type: nonVolatile

Community name: userv1
```

Group name: testv1
Storage-type: nonVolatile

Table 15 Command output

Field	Description
Community name	Displays the community name created by using the snmp-agent community command or the username created by using the snmp-agent usm-user { v1 v2c } command.
Group name	SNMP group name: <ul style="list-style-type: none">• If the community is created by using the snmp-agent community command, the group name is the same as the community name.• If the community is created by using the snmp-agent usm-user { v1 v2c } command, the name of the group to which the user belongs is displayed.
Acl	Number of the ACL that controls the access of the NMSs in the community to the device. Only the NMSs with the IP addresses permitted in the ACL can access the device with the community name.
Storage-type	Storage type: <ul style="list-style-type: none">• volatile—Settings are lost when the system reboots.• nonVolatile—Settings remain after the system reboots.• permanent—Settings remain after the system reboots and can be modified but not deleted.• readOnly—Settings remain after the system reboots and cannot be modified or deleted.• other—Any other storage type.

display snmp-agent group

Syntax

display snmp-agent group [*group-name*] [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

group-name: Specifies an SNMP group name, a case-sensitive string of 1 to 32 characters. You can specify an SNMPv1, SNMPv2c, or SNMPv3 group.

|: 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 snmp-agent group** to display information about an SNMP group, including the group name, security model, MIB view, and storage type. If no group is specified, the command displays information about all SNMP groups.

Examples

Display information about all SNMP groups.

```
<Sysname> display snmp-agent group
  Group name: groupv3
    Security model: v3 noAuthnoPriv
    Readview: ViewDefault
    Writeview: <no specified>
    Notifyview: <no specified>
    Storage-type: nonVolatile
```

Table 16 Command output

Field	Description
Group name	SNMP group name.
Security model	Security model of the SNMP group: <ul style="list-style-type: none">• authPriv—authentication with privacy.• authNoPriv—authentication without privacy.• noAuthNoPriv—no authentication, no privacy. For an SNMPv1 or SNMPv2c group, the security model can be only noAuthNoPriv.
Readview	Read only MIB view accessible to the SNMP group.
Writeview	Writable MIB view associated with the SNMP group.
Notifyview	Notify MIB view for the SNMP group. The SNMP users in the group can send traps only for the nodes in the notify MIB view.
Storage-type	Storage type, including volatile, nonVolatile, permanent, readOnly, and other (see Table 15).

display snmp-agent local-engineid

Syntax

display snmp-agent local-engineid [| { **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 snmp-agent local-engineid** to display the local SNMP engine ID.

The local SNMP engine ID uniquely identifies the SNMP engine of the SNMP agent in an SNMP domain.

Every SNMP agent has one SNMP engine to provide services for sending and receiving messages, authenticating and encrypting messages, and controlling access to managed objects.

Examples

```
# Display the local SNMP engine ID.
```

```
<Sysname> display snmp-agent local-engineid
SNMP local EngineID: 800007DB7F0000013859
```

display snmp-agent mib-view

Syntax

```
display snmp-agent mib-view [ exclude | include | viewname view-name ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

exclude: Displays the subtrees excluded from any MIB view.

include: Displays the subtrees included in any MIB view.

viewname *view-name:* Displays information about the specified MIB view.

| : 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 snmp-agent mib-view** to display MIB view information.

If you do not specify any option, the command displays all MIB views.

Examples

```
# Display all SNMP MIB views of the device.
```

```
<Sysname> display snmp-agent mib-view
```

```
View name:ViewDefault
  MIB Subtree:iso
  Subtree mask:
  Storage-type: nonVolatile
  View Type:included
  View status:active
```

```
View name:ViewDefault
  MIB Subtree:snmpUsmMIB
  Subtree mask:
  Storage-type: nonVolatile
  View Type:excluded
  View status:active
```

```
View name:ViewDefault
  MIB Subtree:snmpVacmMIB
  Subtree mask:
  Storage-type: nonVolatile
  View Type:excluded
  View status:active
```

```
View name:ViewDefault
  MIB Subtree:snmpModules.18
  Subtree mask:
  Storage-type: nonVolatile
  View Type:excluded
  View status:active
```

ViewDefault is the default MIB view. The output shows that all MIB objects in the **iso** subtree are accessible except for the MIB objects in the **snmpUsmMIB**, **snmpVacmMIB**, and **snmpModules.18** subtrees.

Table 17 Command output

Field	Description
View name	MIB view name.
MIB Subtree	MIB subtree covered by the MIB view.
Subtree mask	MIB subtree mask.
Storage-type	Type of the medium where the subtree view is stored.
View Type	Access privilege for the MIB subtree in the MIB view: <ul style="list-style-type: none">• Included—All objects in the MIB subtree are accessible in the MIB view.• Excluded—None of the objects in the MIB subtree is accessible in the MIB view.
View status	Status of the MIB view.

display snmp-agent statistics

Syntax

display snmp-agent 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 snmp-agent statistics** to display SNMP message statistics.

Examples

Display SNMP message statistics.

```
<Sysname> display snmp-agent statistics
1684 Messages delivered to the SNMP entity
5 Messages which were for an unsupported version
0 Messages which used a SNMP community name not known
0 Messages which represented an illegal operation for the community supplied
0 ASN.1 or BER errors in the process of decoding
1679 Messages passed from the SNMP entity
0 SNMP PDUs which had badValue error-status
0 SNMP PDUs which had genErr error-status
0 SNMP PDUs which had noSuchName error-status
0 SNMP PDUs which had tooBig error-status (Maximum packet size 1500)
16544 MIB objects retrieved successfully
2 MIB objects altered successfully
7 GetRequest-PDU accepted and processed
7 GetNextRequest-PDU accepted and processed
1653 GetBulkRequest-PDU accepted and processed
1669 GetResponse-PDU accepted and processed
2 SetRequest-PDU accepted and processed
0 Trap PDUs accepted and processed
0 Alternate Response Class PDUs dropped silently
0 Forwarded Confirmed Class PDUs dropped silently
```

Table 18 Command output

Field	Description
Messages delivered to the SNMP entity	Number of messages that the SNMP agent has received.
Messages which were for an unsupported version	Number of messages that had an SNMP version not configured on the SNMP agent.
Messages which used a SNMP community name not known	Number of messages that has a community name not configured on the SNMP agent.
Messages which represented an illegal operation for the community supplied	Number of messages carrying an operation that the community has no right to perform.
ASN.1 or BER errors in the process of decoding	Number of messages with ASN.1 or BER errors in the process of decoding.
Messages passed from the SNMP entity	Number of messages sent by the SNMP agent.
SNMP PDUs which had badValue error-status	Number of SNMP PDUs with a badValue error.
SNMP PDUs which had genErr error-status	Number of SNMP PDUs with a genErr error.
SNMP PDUs which had noSuchName error-status	Number of PDUs with a noSuchName error.
SNMP PDUs which had tooBig error-status (Maximum packet size 1500)	Number of PDUs with a tooBig error (the maximum packet size is 1500 bytes).
MIB objects retrieved successfully	Number of MIB objects that have been successfully retrieved.
MIB objects altered successfully	Number of MIB objects that have been successfully modified.
GetRequest-PDU accepted and processed	Number of get requests that have been received and processed.
GetNextRequest-PDU accepted and processed	Number of getNext requests that have been received and processed.
GetBulkRequest-PDU accepted and processed	Number of getBulk requests that have been received and processed.
GetResponse-PDU accepted and processed	Number of get responses that have been received and processed.
SetRequest-PDU accepted and processed	Number of set requests that have been received and processed.
Trap PDUs accepted and processed	Number of traps that have been received and processed.
Alternate Response Class PDUs dropped silently	Number of dropped response packets.
Forwarded Confirmed Class PDUs dropped silently	Number of forwarded packets that have been dropped.

display snmp-agent sys-info

Syntax

```
display snmp-agent sys-info [ contact | location | version ] * [ [ { begin | exclude | include } regular-expression ]
```


View

Any view

Default level

1: Monitor level

Parameters

contact: Displays the system contact.

location: Displays the system location.

version: Displays the SNMP version of the SNMP agent.

|: 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 snmp-agent sys-info** to display SNMP system information.

If no keyword is specified, all SNMP agent system information is displayed.

Examples

Display SNMP agent system information.

```
<Sysname> display snmp-agent sys-info
    The contact person for this managed node:

    The physical location of this node:

    SNMP version running in the system:
    SNMPv3
```

display snmp-agent trap queue

Syntax

display snmp-agent trap queue [| { **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 snmp-agent trap queue** to display basic information about the trap queue, including trap queue name, queue length and the number of traps in the queue currently.

Related commands: **snmp-agent trap life** and **snmp-agent trap queue-size**.

Examples

Display the current configuration and usage of the trap queue.

```
<Sysname> display snmp-agent trap queue
Queue name: SNTP
Queue size: 100
Message number: 6
```

Table 19 Command output

Field	Description
Queue name	Trap queue name
Queue size	Trap queue size
Message number	Number of traps in the current trap queue

display snmp-agent trap-list

Syntax

display snmp-agent trap-list [| { **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 snmp-agent trap-list** to display modules that can generate traps and their trap status (**enable** or **disable**).

You can use the **snmp-agent trap enable** command to enable or disable the trap function of a module. For a module that has multiple sub-modules, the trap status is **enable** if the trap function of any of its sub-modules is enabled.

Related commands: **snmp-agent trap enable**.

Examples

```
# Display the modules that can generate traps and their trap status.
```

```
<Sysname> display snmp-agent trap-list
  arp trap enable
  configuration trap enable
  flash trap enable
  standard trap enable
  system trap enable
```

```
Enable traps: 5; Disable traps: 0
```

display snmp-agent usm-user

Syntax

```
display snmp-agent usm-user [ engineid engineid | username user-name | group group-name ] * [ |
{ begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

engineid *engineid*: Displays SNMPv3 user information for the SNMP engine ID identified by *engineid*. When an SNMPv3 user is created, the system records the current local SNMP entity engine ID. The user becomes invalid when the engine ID changes and becomes valid again when the recorded engine ID is restored.

username *user-name*: Displays information about an SNMPv3 user. The username is case-sensitive.

group *group-name*: Displays SNMPv3 user information for an SNMP group name. The group name is case-sensitive.

|: 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 snmp-agent usm-user** to display SNMPv3 user information.

Examples

```
# Display information about SNMPv3 users.
```

```
<Sysname> display snmp-agent usm-user
  User name: userv3
  Group name: mygroupv3
```

```
Engine ID: 800063A203000FE240A1A6
Storage-type: nonVolatile
UserStatus: active
```

```
User name: userv3code
Group name: groupv3code
Engine ID: 800063A203000FE240A1A6
Storage-type: nonVolatile
UserStatus: active
```

Table 20 Command output

Field	Description
User name	SNMP username.
Group name	SNMP group name.
Engine ID	Engine ID for an SNMP entity.
Storage-type	Storage type: <ul style="list-style-type: none">• volatile• nonvolatile• permanent• readOnly• other For more information, see Table 15 .
UserStatus	SNMP user status.

enable snmp trap updown

Syntax

enable snmp trap updown

undo enable snmp trap updown

View

Interface view

Default level

2: System level

Parameters

None

Description

Use **enable snmp trap updown** to enable link state traps on an interface.

Use **undo enable snmp trap updown** to disable link state traps on an interface.

By default, link state traps are enabled.

For an interface to generate linkUp/linkDown traps when its state changes, you must also enable the linkUp/linkDown trap function globally by using the **enable snmp trap updown** command.

Related commands: **snmp-agent target-host** and **snmp-agent trap enable**.

Examples

```
# Enable port GigabitEthernet 1/0/1 to send linkUp/linkDown SNMP traps to 10.1.1.1 in the community public.
```

```
<Sysname> system-view
[Sysname] snmp-agent trap enable
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] enable snmp trap updown
```

snmp-agent

Syntax

snmp-agent

undo snmp-agent

View

System view

Default level

3: Manage level

Parameters

None

Description

Use **snmp-agent** to enable the SNMP agent.

Use **undo snmp-agent** to disable the SNMP agent.

By default, the SNMP agent is disabled.

The **snmp-agent** command is optional for an SNMP configuration task. The SNMP agent is automatically enabled when you perform any command that begins with **snmp-agent** except for the **snmp-agent calculate-password** and **snmp-agent ifmib long-ifindex enable** commands.

Examples

```
# Enable the SNMP agent.
```

```
<Sysname> system-view
[Sysname] snmp-agent
```

snmp-agent calculate-password

Syntax

In non-FIPS mode:

```
snmp-agent calculate-password plain-password mode { 3desmd5 | 3dessha | md5 / sha }
{ local-engineid | specified-engineid engineid }
```

In FIPS mode:

```
snmp-agent calculate-password plain-password mode sha { local-engineid | specified-engineid engineid }
```

View

System view

Default level

3: Manage level

Parameters

plain-password: Specifies a plaintext authentication or privacy key.

mode: Specifies authentication and privacy algorithms. Select a mode option, depending on the authentication and privacy algorithm you are configuring with the **snmp-agent usm-user v3** command. The three privacy algorithms Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), and Data Encryption Standard (DES) are in descending order of security strength. Higher security means more complex implementation mechanism and lower speed. DES is enough to meet general requirements. The Message-Digest Algorithm 5 (MD5) and Secure Hash Algorithm (SHA-1) are the two authentication algorithms. MD5 is faster but less secure than SHA-1.

- **3desmd5**: Converts the plaintext privacy key to an encrypted key for 3DES encryption used together with MD5 authentication.
- **3dessha**: Converts the plaintext privacy key to an encrypted key for 3DES encryption used together with SHA-1 authentication.
- **md5**: Converts the plaintext authentication key to an encrypted key for MD5 authentication, or converts the plaintext privacy key to an encrypted key for AES or DES encryption used in conjunction with MD5.
- **sha**: Converts the plaintext authentication key to an encrypted key for SHA-1 authentication, or converts the plaintext privacy key to an encrypted key for AES or DES encryption used in conjunction with SHA-1 authentication.

local-engineid: Uses the local engine ID to calculate the encrypted key. For more information about engine ID-related configuration, see the **snmp-agent local-engineid** command.

specified-engineid: Uses a user-defined engine ID to calculate the cipher text password.

engineid: Specifies an SNMP engine ID as a hexadecimal string. It must comprise an even number of hexadecimal characters, in the range of 10 to 64. All-zero and all-F strings are invalid.

Description

Use **snmp-agent calculate-password** to convert a plaintext key to an encrypted key for authentication or encryption.

This command helps you calculate encrypted authentication and privacy keys for SNMPv3 users that use encrypted authentication and privacy keys. To create an SNMPv3 user, see the **snmp-agent usm-user v3** command.

Make sure the SNMP agent is enabled before you execute the **snmp-agent calculate-password** command.

The converted key is valid only under the engine ID specified for key conversion.

Related commands: **snmp-agent usm-user v3**.

Examples

Use the local engine and the MD5 algorithm to convert the plaintext key **authkey** to an encrypted key.

```
<Sysname> system-view
[Sysname] snmp-agent calculate-password authkey mode md5 local-engineid
The secret key is: 09659EC5A9AE91BA189E5845E1DDE0CC
```

snmp-agent community

Syntax

snmp-agent community { **read** | **write** } *community-name* [**mib-view** *view-name*] [**acl** *acl-number* | **acl** **ipv6** *ipv6-acl-number*] *

undo snmp-agent community { **read** | **write** } *community-name*

View

System view

Default level

3: Manage level

Parameters

read: Assigns the specified community the read only access to MIB objects. A read-only community can only inquire MIB information.

write: Assigns the specified community the read and write access to MIB objects. A read and write community can configure MIB information.

community-name: Specifies the community name, a string of 1 to 32 characters.

mib-view *view-name*: Specifies the MIB view available for the community. The *view-name* argument represents a MIB view name, which is a string of 1 to 32 characters. A MIB view represents a set of accessible MIB objects. If no MIB view is specified, the specified community can access the MIB objects in the default MIB view **ViewDefault**. To create a MIB view, use the **snmp-agent mib-view** command.

acl *acl-number*: Specifies a basic ACL to filter NMSs by source IPv4 address. The *acl-number* argument represents a basic ACL number in the range of 2000 to 2999. Only the NMSs with the IP addresses permitted in the ACL can use the specified community name to access the SNMP agent.

acl ipv6 *ipv6-acl-number*: Specifies a basic ACL to filter NMSs by source IPv6 address. The *ipv6-acl-number* argument represents a basic ACL number in the range of 2000 to 2999. Only the NMSs with the IPv6 addresses permitted in the ACL can use the community name to access the SNMP agent.

Description

Use **snmp-agent community** to configure an SNMP community.

Use **undo snmp-agent community** to delete an SNMP community.

This command is for SNMPv1 and SNMPv2c. It is supported only in non-FIPS mode.

A community comprises NMSs and SNMP agents, and is identified by a community name. When devices in a community communicate with each other, they use the community name for authentication. An NMS and an SNMP agent can access each other only when they are configured with the same community name. Typically, **public** is used as the read-only community name, and **private** is used as the read and write community name. To improve security, assign your SNMP communities a name other than **public** and **private**.

To make sure the MIB objects are accessible only to a specific NMS, use a basic ACL to identify the source IP address of the NMS. To set the range of the MIB objects available for the community, use a MIB view.

Related commands: **snmp-agent mib-view**.

Examples

Create the read-only community **readaccess** so an NMS can use the protocol SNMPv1 or SNMPv2c and community name **readaccess** to read the MIB objects in the default view **ViewDefault**.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v1 v2c
[Sysname] snmp-agent community read readaccess
```

Create the read and write community **writeaccess** so only the host at 1.1.1.1 can use the protocol SNMPv2c and community name **writeaccess** to read and set the MIB objects in the default view **ViewDefault**.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 1.1.1.1 0.0.0.0
[Sysname-acl-basic-2001] rule deny source any
[Sysname-acl-basic-2001] quit
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent community write writeaccess acl 2001
```

Create the read and write community **wr-sys-acc** so an NMS can use the protocol SNMPv1 or SNMPv2c, community name **wr-sys-acc** to read and set the MIB objects in the system subtree (OID 1.3.6.1.2.1.1).

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v1 v2c
[Sysname] undo snmp-agent mib-view ViewDefault
[Sysname] snmp-agent mib-view included test system
[Sysname] snmp-agent community write wr-sys-acc mib-view test
```

snmp-agent group

Syntax

SNMPv1 and SNMP v2c:

```
snmp-agent group { v1 | v2c } group-name [ read-view view-name ] [ write-view view-name ]
[ notify-view view-name ] [ acl acl-number | acl ipv6 ipv6-acl-number ] *
```

```
undo snmp-agent group { v1 | v2c } group-name
```

SNMPv3:

```
snmp-agent group v3 group-name [ authentication | privacy ] [ read-view view-name ] [ write-view
view-name ] [ notify-view view-name ] [ acl acl-number | acl ipv6 ipv6-acl-number ] *
```

```
undo snmp-agent group v3 group-name [ authentication | privacy ]
```

View

System view

Default level

3: Manage level

Parameters

v1: Specifies SNMPv1.

v2c: Specifies SNMPv2c.

v3: Specifies SNMPv3.

group-name: Specifies the group name, a string of 1 to 32 characters.

authentication: Specifies the security model of the SNMPv3 group to be authentication only (without privacy).

privacy: Specifies the security model of the SNMPv3 group to be authentication and privacy.

read-view *view-name*: Specifies a read-only MIB view. The *view-name* represents a MIB view, which is a string of 1 to 32 characters. The users in the specified group have read only access to the objects included in the MIB view. The default read view is **ViewDefault**.

write-view *view-name*: Specifies a read and write MIB view. The *view-name* argument represents a MIB view, which is a string of 1 to 32 characters. The users in the specified group have read and write access to the objects included in the MIB view. By default, no write view is configured, which means the NMS cannot perform the write operations to all MIB objects on the device.

notify-view *view-name*: Specifies a trap MIB view. The *view-name* argument represents a MIB view, which is a string of 1 to 32 characters. The system sends traps to the users in the specified group for the objects included in the MIB view. By default, no notify view is configured, which means the agent does not send traps to the NMS.

acl *acl-number*: Specifies a basic ACL to filter NMSs by source IPv4 address. The *acl-number* argument represents a basic ACL number in the range of 2000 to 2999. In the specified SNMP group, only the NMSs with the IP addresses permitted in the ACL can access the SNMP agent.

acl ipv6 *ipv6-acl-number*: Specifies a basic ACL to filter NMSs by source IPv6 address. The *ipv6-acl-number* argument represents a basic ACL number in the range of 2000 to 2999. In the specified SNMP group, only the NMSs with the IPv6 addresses permitted in the ACL can access the SNMP agent.

Description

Use **snmp-agent group** to create an SNMP group and specify its access right.

Use **undo snmp-agent group** to delete an SNMP group.

By default, no SNMP group exists. SNMPv3 groups use the no authentication, no privacy security model if neither **authentication** nor **privacy** is specified.

All the users in an SNMP group share the security model and access rights of the group.

The **snmp-agent group { v1 | v2c }** command is supported only in non-FIPS mode.

Related commands: **snmp-agent mib-view** and **snmp-agent usm-user**.

Examples

Create the SNMPv3 group **group1** and assign the no authentication, no privacy security model to the group.

```
<Sysname> system-view
[Sysname] snmp-agent group v3 group1
```

snmp-agent local-engineid

Syntax

snmp-agent local-engineid *engineid*

undo snmp-agent local-engineid

View

System view

Default level

3: Manage level

Parameters

engineid: Specifies an SNMP engine ID as a hexadecimal string. It must comprise an even number of hexadecimal characters, in the range of 10 to 64. All-zero and all-F strings are invalid.

Description

Use **snmp-agent local-engineid** to configure the SNMP engine ID of the local SNMP agent.

Use **undo snmp-agent local-engineid** to restore the default local SNMP engine ID.

By default, the local engine ID is the combination of the company ID and the device ID. Device ID varies by product and might be an IP address, a MAC address, or a user-defined hexadecimal string.

An SNMP engine ID uniquely identifies an SNMP entity in an SNMP managed network. Make sure the local SNMP engine ID is unique within your SNMP managed network to avoid communication problems.

If you have configured SNMPv3 users, change the local SNMP engine ID only when necessary. The change can void the SNMPv3 usernames and encrypted keys you have configured.

Related commands: **snmp-agent usm-user**.

Examples

```
# Configure the local engine ID as 123456789A.  
<Sysname> system-view  
[Sysname] snmp-agent local-engineid 123456789A
```

snmp-agent log

Syntax

```
snmp-agent log { all | get-operation | set-operation }  
undo snmp-agent log { all | get-operation | set-operation }
```

View

System view

Default level

3: Manage level

Parameters

all: Enables logging SNMP Get and Set operations.

get-operation: Enables logging SNMP Get operations.

set-operation: Enables logging SNMP Set operations.

Description

Use **snmp-agent log** to enable SNMP logging.

Use **undo snmp-agent log** to restore the default.

By default, SNMP logging is disabled.

Use SNMP logging to record the SNMP operations performed on the SNMP agent for auditing NMS behaviors. The SNMP agent sends log data to the information center. You can configure the information center to output the data to a specific destination as needed.

Examples

```
# Enable logging SNMP GET operations.
<Sysname> system-view
[Sysname] snmp-agent log get-operation

# Enable logging SNMP SET operations.
<Sysname> system-view
[Sysname] snmp-agent log set-operation
```

snmp-agent ifmib long-ifindex enable

Syntax

```
snmp-agent ifmib long-ifindex enable
undo snmp-agent ifmib long-ifindex enable
```

View

System view

Default level

2: System level

Parameters

None

Description

Use **snmp-agent ifmib long-ifindex enable** to switch the format of an NM-specific ifindex from 16-bit to 32-bit.

Use **undo snmp-agent ifmib long-ifindex enable** to restore the default.

By default, an NM-specific ifindex is in 16-bit format.

Some configurations use parameters relating to NM-specific ifindex; therefore, the switch of NM-specific ifindex causes temporary ineffectiveness of these configurations (if the format of the ifindex is switched back, the configurations will become effective again). In this case, you need to perform the configurations again with the new NM-specific ifindexes, and then the related configurations become effective. For example, in the configuration of RMON alarm group and private alarm group, the alarm variables are presented in the format of **OID/variable-name.NM-specific-ifindex**; the switching of NM-specific ifindex format makes the RMON alarm variables ineffective. To monitor the affected nodes again, you need to re-configure the alarm groups with the new format of NM-specific ifindexes.

Examples

```
# Switch the format of an NM-specific ifindex from 16-bit to 32-bit.
<Sysname> system-view
[Sysname] snmp-agent ifmib long-ifindex enable
```

snmp-agent mib-view

Syntax

```
snmp-agent mib-view { excluded | included } view-name oid-tree [ mask mask-value ]  
undo snmp-agent mib-view view-name
```

View

System view

Default level

3: Manage level

Parameters

excluded: Denies access to any node in the specified MIB subtree.

included: Permits access to the nodes in the specified MIB subtree.

view-name: Specifies the view name, a string of 1 to 32 characters.

oid-tree: Specifies a MIB subtree by its root node's OID (for example **1.4.5.3.1**) or object name (for example, **system**). An OID is a dotted numeric string that uniquely identifies an object in the MIB tree.

mask mask-value: Sets a MIB subtree mask, a hexadecimal string. Its length must be an even number in the range of 2 to 32. For example, you can specify **0a**, **aa**, but not **0aa**. If no subtree mask is specified, the MIB subtree mask is an all-F hexadecimal string. The MIB subtree and the subtree mask together identify a set of objects to be included or excluded from the view.

Description

Use **snmp-agent mib-view** to create or update a MIB view.

Use **undo snmp-agent mib-view** to delete a MIB view.

By default, the system creates the **ViewDefault** view when the SNMP agent is enabled. In the default MIB view, all MIB objects in the **iso** subtree but the **snmpUsmMIB**, **snmpVacmMIB**, and **snmpModules.18** subtrees are accessible.

A MIB view represents a set of MIB objects (or MIB object hierarchies) with certain access privilege. The MIB objects included in the MIB view are accessible while those excluded from the MIB view are inaccessible.

Each *view-name oid-tree* pair represents a view record. If you specify the same record with different MIB subtree masks multiple times, the last configuration takes effect.

The system can store entries for up to 20 unique MIB view records. In addition to the four default MIB view records, you can create up to 16 unique MIB view records. After you delete the default view with the **undo snmp-agent mib-view** command, you can create up to 20 unique MIB view records.

Be cautious with deleting the default MIB view. The operation blocks access to any MIB object on the device from NMSs that use the default view.

Related commands: **snmp-agent community** and **snmp-agent group**.

Examples

```
# Include the mib-2 (OID 1.3.6.1) subtree in the mibtest view and exclude the ip subtree from this view.  
<Sysname> system-view  
[Sysname] snmp-agent mib-view included mibtest 1.3.6.1  
[Sysname] snmp-agent mib-view excluded mibtest ip
```

```
[Sysname] snmp-agent community read public mib-view mibtest
```

An SNMPv1 NMS in the **public** community can query the objects in the **mib-2** subtree, but not any object (for example, the **ipForwarding** or **ipDefaultTTL** node) in the **ip** subtree.

snmp-agent packet max-size

Syntax

snmp-agent packet max-size *byte-count*

undo snmp-agent packet max-size

View

System view

Default level

3: Manage level

Parameters

byte-count: Specifies the maximum size (in bytes) of SNMP packets that the SNMP agent can receive or send. The value range is 484 to 17940, and the default is 1500.

Description

Use **snmp-agent packet max-size** to set the maximum size (in bytes) of SNMP packets that the SNMP agent can receive or send.

Use **undo snmp-agent packet max-size** to restore the default packet size.

By default, the maximum size of SNMP packets is 1500 bytes.

If any device on the path to the NMS does not support packet fragmentation, limit the SNMP packet size to prevent large-sized packets from being discarded. For most networks, the default value is sufficient.

Examples

```
# Set the maximum SNMP packet size to 1024 bytes.
```

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

```
[Sysname] snmp-agent packet max-size 1024
```

snmp-agent packet response dscp

Syntax

snmp-agent packet response dscp *dscp-value*

undo snmp-agent packet response dscp

View

System view

Default level

3: Manage level

Parameters

dscp-value: Specifies the DSCP value for SNMP responses, in the range of 0 to 63.

Description

Use **snmp-agent packet response dscp** to set the DSCP value for SNMP responses.

Use **undo snmp-agent packet response dscp** to restore the default.

The default DSCP value for SNMP responses is 0.

Examples

Set the DSCP value to 45 for SNMP responses.

```
<Sysname> system-view
[Sysname] snmp-agent packet response dscp 45
```

snmp-agent sys-info

Syntax

In non-FIPS mode:

```
snmp-agent sys-info { contact sys-contact | location sys-location | version { all | { v1 | v2c | v3 }* } }
undo snmp-agent sys-info { contact | location | version { all | { v1 | v2c | v3 }* } }
```

In FIPS mode:

```
snmp-agent sys-info { contact sys-contact | location sys-location | version v3 }
undo snmp-agent sys-info { contact | location | version v3 }
```

View

System view

Default level

3: Manage level

Parameters

contact *sys-contact*: Specifies the system contact, a string of 1 to 200 characters.

location *sys-location*: Specifies the system location, a string of 1 to 200 characters. This information is stored in a management variable in the **system** group defined in RFC1213-MIB.

version: Specifies SNMP versions.

- **all**: Specifies SNMPv1, SNMPv2c, and SNMPv3. This keyword is supported only in non-FIPS mode.
- **v1**: Specifies SNMPv1. This keyword is supported only in non-FIPS mode.
- **v2c**: Specifies SNMPv2c. This keyword is supported only in non-FIPS mode.
- **v3**: Specifies SNMPv3.

Description

Use **snmp-agent sys-info** to configure system information for the SNMP agent, including the contact, location, and SNMP versions.

Use **undo snmp-agent sys-info contact** and **undo snmp-agent sys-info location** to restore the default.

Use **undo snmp-agent sys-info version** to disable an SNMP version.

By default, the location is null, the SNMP version is **SNMPv3**, and the contact is null.

Configure the SNMP agent with the same SNMP version as the NMS for successful communications between them.

Related commands: **display snmp-agent sys-info**.

Examples

Configure the system contact as **Dial System Operator at beeper # 27345**.

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

```
[Sysname] snmp-agent sys-info contact Dial System Operator at beeper # 27345
```

snmp-agent target-host

Syntax

In non-FIPS mode:

```
snmp-agent target-host trap address udp-domain { ip-address | ipv6 ipv6-address } [ udp-port port-number ] [ dscp dscp-value ] params securityname security-string [ v1 | v2c | v3 [ authentication | privacy ] ]
```

```
undo snmp-agent target-host trap address udp-domain { ip-address | ipv6 ipv6-address } params securityname security-string
```

In FIPS mode:

```
snmp-agent target-host trap address udp-domain { ip-address | ipv6 ipv6-address } [ udp-port port-number ] [ dscp dscp-value ] params securityname security-string v3 [ authentication | privacy ]
```

```
undo snmp-agent target-host trap address udp-domain { ip-address | ipv6 ipv6-address } params securityname security-string
```

View

System view

Default level

3: Manage level

Parameters

trap: Specifies a target host for receiving the traps sent by the SNMP agent.

address: Specifies the IP address of the trap target host.

udp-domain: Specifies UDP as the transport protocol.

ip-address: Specifies the IPv4 address of the target host.

ipv6 *ipv6-address*: Specifies the IPv6 address of the target host.

udp-port *port-number*: Specifies the UDP port for receiving SNMP traps. The default UDP port is 162.

dscp *dscp-value*: Sets the DSCP value for SNMP traps. The value range is 0 to 63 and the default DSCP is 0.

params securityname *security-string*: Specifies the authentication related parameter. The *security-string* argument specifies an SNMPv1 or SNMPv2c community name or an SNMPv3 username, a string of 1 to 32 characters.

v1: Specifies SNMPv1. This keyword is supported only in non-FIPS mode.

v2c: Specifies SNMPv2c. This keyword is supported only in non-FIPS mode.

v3: Specifies SNMPv3.

- **authentication**: Specifies the security model to be authentication without privacy. You must specify the authentication key when you create the SNMPv3 user.
- **privacy**: Specifies the security model to be authentication with privacy. You must specify the authentication key and privacy key when you create the SNMPv3 user.

Description

Use **snmp-agent target-host** to configure a target host for receiving traps sent by the SNMP agent.

Use **undo snmp-agent target-host** to remove settings for an SNMP trap target host.

You can specify up to 20 trap target hosts.

Make sure the SNMP agent uses the same UDP port number as the target host for traps. If **udp-port port-number** is not specified, UDP port 162 is used by default. Port 162 is the SNMP-specified port used for receiving traps, and is used by most NMSs, including IMC and MIB Browser.

Make sure the SNMP agent uses the same SNMP version as the trap target host so the host can receive traps. If none of the keywords **v1**, **v2c**, or **v3** is specified, SNMPv1 is used.

If neither **authentication** nor **privacy** is specified, the authentication mode is no authentication, no privacy.

In non-FIPS mode, if none of the keywords **v1**, **v2c**, or **v3** is specified, SNMPv1 is used.

In FIPS mode, **v3** must be specified.

Related commands: **enable snmp trap updown**, **snmp-agent trap enable**, **snmp-agent trap life**, and **snmp-agent trap source**.

Examples

Configure the SNMP agent to send SNMPv1 traps to 10.1.1.1 in the community **public**.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable standard
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public
```

snmp-agent trap enable

Syntax

snmp-agent trap enable [**arp rate-limit** | **configuration** | **default-route** | **flash** | **standard** | **authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]* [**system**]

undo snmp-agent trap enable [**arp rate-limit** | **configuration** | **default-route** | **flash** | **standard** | **authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]* [**system**]

View

System view

Default level

3: Manage level

Parameters

arp rate-limit: Enables ARP rate limit traps, which are sent when the ARP packet rate exceeds the rate limit.

configuration: Enables configuration traps.

flash: Enables Flash-related SNMP traps.

default-route: Enables default route traps, which are sent when default routes are deleted.

standard: Enables the sending of standard traps.

- **authentication:** Enables sending authentication failure traps in the event of authentication failure.
- **coldstart:** Sends coldstart traps when the device restarts.
- **linkdown:** Globally enables sending LinkDown traps when the link of a port goes down.
- **linkup:** Globally enables sending LinkUp traps when the link of a port goes up.
- **warmstart:** Sends warmstart traps when the SNMP agent restarts.

system: Enables system event (private MIB) traps.

Description

Use **snmp-agent trap enable** to enable traps globally.

Use **undo snmp-agent trap enable** to disable traps globally.

By default, traps are enabled for all modules.

After you globally enable a trap function for a module, whether the module generates traps also depends on the configuration of the module. For more information, see the sections for each module.

To generate Linkup or Linkdown traps when the link state of an interface changes, you must enable the linkUp or linkDown trap function globally by using the **snmp-agent trap enable [standard [linkdown | linkup] *]** command and on the interface by using the **enable snmp trap updown** command.

Related commands: **snmp-agent target-host** and **enable snmp trap updown**.

Examples

```
# Enable the SNMP agent to send SNMP authentication failure traps to 10.1.1.1 in the community public.
<Sysname> system-view
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public
[Sysname] snmp-agent trap enable standard authentication
```

snmp-agent trap if-mib link extended

Syntax

snmp-agent trap if-mib link extended

undo snmp-agent trap if-mib link extended

View

System view

Default level

3: Manage level

Parameters

None

Description

Use **snmp-agent trap if-mib link extended** to configure the SNMP agent to send extended linkUp/linkDown traps.

Use **undo snmp-agent trap if-mib link extended** to restore the default.

By default, the SNMP agent sends standard linkUp/linkDown traps.

The extended linkUp and linkDown traps adds interface description and interface type to the standard linkUp and linkDown traps for fast failure point identification. When you configure the **snmp-agent trap if-mib link extended** command, make sure the NMS supports the extended linkUp and linkDown traps.

- A standard linkUp trap is in the following format:

```
#Jan 24 11:48:04:896 2011 Sysname IFNET/4/INTERFACE UPDOWN:
Trap 1.3.6.1.6.3.1.1.5.4<linkUp>: Interface 983555 is Up, ifAdminStatus is 1,
ifOperStatus is 1
```

- An extended linkUp trap is in the following format:

```
#Jan 24 11:43:09:896 2011 Sysname IFNET/4/INTERFACE UPDOWN:
Trap 1.3.6.1.6.3.1.1.5.4<linkUp>: Interface 983555 is Up, ifAdminStatus is 1,
ifOperStatus is 1, ifDescr is Ethernet1/1, ifType is 6
```

- A standard linkDown trap is in the following format:

```
#Jan 24 11:47:35:224 2011 Sysname IFNET/4/INTERFACE UPDOWN:
Trap 1.3.6.1.6.3.1.1.5.3<linkDown>: Interface 983555 is Down, ifAdminStatus is 2,
ifOperStatus is 2
```

- An extended linkDown trap is in the following format:

```
#Jan 24 11:42:54:314 2011 AR29.46 IFNET/4/INTERFACE UPDOWN:
Trap 1.3.6.1.6.3.1.1.5.3<linkDown>: Interface 983555 is Down, ifAdminStatus is 2,
ifOperStatus is 2, ifDescr is GigabitEthernet1/0/1, ifType is 6
```

The format of an extended linkup/ linkDown trap is the standard format followed with the ifDescr and ifType information, facilitating problem location.

When this command is configured, the device sends extended linkUp/linkDown traps. If the extended messages are not supported on NMS, the device may not be able to resolve the messages.

Examples

Extend standard linkUp/linkDown traps.

```
<Sysname> system-view
[Sysname] snmp-agent trap if-mib link extended
```

snmp-agent trap life

Syntax

snmp-agent trap life *seconds*

undo snmp-agent trap life

View

System view

Default level

3: Manage level

Parameters

seconds: Specifies the timeout time in the range of 1 to 2592000 seconds.

Description

Use **snmp-agent trap life** to configure the holding time of the traps in the queue. Traps are discarded when the holding time expires.

Use **undo snmp-agent trap life** to restore the default holding time of traps in the queue.

By default, the holding time of SNMP traps in the queue is 120 seconds.

The SNMP module sends traps in queues. As soon as the traps are saved in the trap queue, a timer is started. If traps are not sent out until the timer times out (in other words, the holding time configured by using this command expires), the system removes the traps from the trap sending queue.

Related commands: **snmp-agent trap enable** and **snmp-agent target-host**.

Examples

```
# Configure the holding time of traps in the queue as 60 seconds.
```

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

```
[Sysname] snmp-agent trap life 60
```

snmp-agent trap queue-size

Syntax

snmp-agent trap queue-size *size*

undo snmp-agent trap queue-size

View

System view

Default level

3: Manage level

Parameters

size: Specifies the number of traps that can be stored in the trap sending queue, in the range of 1 to 1000.

Description

Use **snmp-agent trap queue-size** to set the size of the trap sending queue.

Use **undo snmp-agent trap queue-size** to restore the default queue size.

By default, up to 100 traps can be stored in the trap sending queue.

Traps are saved into the trap sending queue when generated. The size of the queue determines the maximum number of traps that can be stored in the queue. When the size of the trap sending queue reaches the configured value, the newly generated traps are saved into the queue, and the earliest ones are discarded.

Related commands: **snmp-agent target-host**, **snmp-agent trap enable**, and **snmp-agent trap life**.

Examples

```
# Set the maximum number of traps that can be stored in the trap sending queue to 200.
```

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

```
[Sysname] snmp-agent trap queue-size 200
```

snmp-agent trap source

Syntax

snmp-agent trap source *interface-type interface-number*

undo snmp-agent trap source

View

System view

Default level

3: Manage level

Parameters

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

Description

Use **snmp-agent trap source** to specify the source IP address contained in the traps.

Use **undo snmp-agent trap source** to restore the default.

By default, SNMP chooses the IP address of an interface to be the source IP address of the traps.

Upon the execution of this command, the system uses the primary IP address of the specified interface as the source IP address of the traps, and the NMS uses this IP address to uniquely identify the agent. Even if the agent sends out traps through different interfaces, the NMS uses this IP address to filter all traps sent from the agent.

Before you can configure the IP address of a particular interface as the source IP address of the trap, make sure the interface already exists and that it has a legal IP address. If the configured interface does not exist, the configuration fails. If the specified IP address is illegal, the configuration becomes invalid. When a legal IP address is configured for the interface, the configuration automatically becomes valid.

Related commands: **snmp-agent target-host** and **snmp-agent trap enable**.

Examples

Configure the IP address for the port Vlan-interface1 as the source address for traps.

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

```
[Sysname] snmp-agent trap source Vlan-interface1
```

snmp-agent usm-user { v1 | v2c }

Syntax

snmp-agent usm-user { v1 | v2c } *user-name group-name* [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*]
*

undo snmp-agent usm-user { v1 | v2c } *user-name group-name*

View

System view

Default level

3: Manage level

Parameters

v1: Specifies SNMPv1.

v2c: Specifies SNMPv2c.

user-name: Specifies the username, a case-sensitive string of 1 to 32 characters.

group-name: Specifies the group name, a case-sensitive string of 1 to 32 characters. The group can be one that has been created or not. If the group has not been created, the user takes effect after you create the group.

acl acl-number: Specifies a basic ACL to filter NMSs by source IPv4 address. The *acl-number* argument represents a basic ACL number in the range of 2000 to 2999. Only the NMSs with the IPv4 addresses permitted in the ACL can use the specified username (community name) to access the SNMP agent.

acl ipv6 ipv6-acl-number: Specifies a basic ACL to filter NMSs by source IPv6 address. The *ipv6-acl-number* argument represents a basic ACL number in the range of 2000 to 2999. Only the NMSs with the IPv6 addresses permitted in the ACL can use the specified username (community name) to access the SNMP agent.

Description

Use **snmp-agent usm-user { v1 | v2c }** to add a user to an SNMPv1 or SNMPv2c group.

Use **undo snmp-agent usm-user { v1 | v2c }** to delete a user from an SNMPv1 or SNMPv2c group.

When you create an SNMPv1 or SNMPv2c user, the system automatically creates a read-only community that has the same name as the SNMPv1 or SNMPv2c username. To change the access right of this community to write access, use the **snmp-agent community** command or the **snmp-agent group { v1 | v2c }** command. To display the SNMPv1 and SNMPv2c communities created in this way, use the **display snmp-agent community** command.

The **snmp-agent usm-user { v1 | v2c }** command enables managing SNMPv1 and SNMPv2c users in the same way as managing SNMPv3 users. It does not affect the way of configuring SNMPv1 and SNMPv2c communities on the NMS.

Make sure you have created the SNMPv1 or SNMPv2c group.

This command is supported only in non-FIPS mode.

Related commands: **snmp-agent community** and **snmp-agent group**.

Examples

Add the user **userv2c** to the SNMPv2c group **readCom** so an NMS can use the protocol SNMPv2c and the read-only community name **userv2c** to access the SNMP agent.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent group v2c readCom
[Sysname] snmp-agent usm-user v2c userv2c readCom
```

Add the user **userv2c** in the SNMPv2c group **readCom** so only the NMS at 1.1.1.1 can use the protocol SNMPv2c and read-only community name **userv2c** to access the SNMP agent.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 1.1.1.1 0.0.0.0
[Sysname-acl-basic-2001] rule deny source any
[Sysname-acl-basic-2001] quit
[Sysname] snmp-agent sys-info version v2c
```

```
[Sysname] snmp-agent group v2c readCom
[Sysname] snmp-agent usm-user v2c userv2c readCom acl 2001
```

snmp-agent usm-user v3

Syntax

In non-FIPS mode:

```
snmp-agent usm-user v3 user-name group-name [ cipher ] [ authentication-mode { md5 | sha }
auth-password [ privacy-mode { 3des | aes128 | des56 } priv-password ] [ acl acl-number | acl ipv6
ipv6-acl-number ] *
```

```
undo snmp-agent usm-user v3 user-name group-name { local | engineid engineid-string }
```

In FIPS mode:

```
snmp-agent usm-user v3 user-name group-name [ cipher ] [ authentication-mode sha auth-password
[ privacy-mode aes128 priv-password ] ] [ acl acl-number | acl ipv6 ipv6-acl-number ] *
```

```
undo snmp-agent usm-user v3 user-name group-name { local | engineid engineid-string }
```

View

System view

Default level

3: Manage level

Parameters

user-name: Specifies the username, a case-sensitive string of 1 to 32 characters.

group-name: Specifies the group name, a case-sensitive string of 1 to 32 characters.

cipher: Sets ciphertext authentication and privacy keys. If this keyword is not specified, *auth-password* and *priv-password* must be plaintext keys. To obtain the hexadecimal ciphertext for a key, use the **snmp-agent calculate-password** command.

authentication-mode: Specifies an authentication algorithm. MD5 is faster but less secure than SHA. For more information about these algorithms, see *Security Configuration Guide*.

- **md5**: Specifies the MD5 authentication algorithm. This keyword is supported only in non-FIPS mode.
- **sha**: Specifies the SHA-1 authentication protocol algorithm.

auth-password: Specifies the authentication key string. This argument is case sensitive. If **cipher** is not specified, it must be a plaintext string of 1 to 64 characters. If **cipher** is specified, the ciphertext key length requirements differ by authentication algorithm and key string format, as shown in [Table 21](#).

Table 21 Encrypted authentication key length requirements

Authentication algorithm	Hexadecimal string	Non-hexadecimal string
MD5	32 characters	53 characters
SHA	40 characters	57 characters

privacy-mode: Specifies an encryption algorithm for privacy. The three encryption algorithms AES, 3DES, and DES are in descending order of security. Higher security means more complex implementation mechanism and lower speed. DES is enough to meet general requirements.

- **3des**: Specifies the 3DES algorithm. This keyword is supported only in non-FIPS mode.
- **des56**: Specifies the DES algorithm. This keyword is supported only in non-FIPS mode.
- **aes128**: Specifies the AES algorithm.

priv-password: Specifies the privacy key string. This argument is case sensitive. If **cipher** is not specified, it must be a plaintext string of 1 to 64 characters. If **cipher** is specified, the ciphertext key length requirements differ by authentication algorithm and key string format, as shown in [Table 22](#).

Table 22 Encrypted privacy key length requirements

Authentication algorithm	Encryption algorithm	Hexadecimal string	Non-hexadecimal string
MD5	3DES	64 characters	73 characters
MD5	AES128 or DES-56	32 characters	53 characters
SHA	3DES	80 characters	73 characters
SHA	AES128 or DES-56	40 characters	53 characters

acl *acl-number*: Specifies a basic ACL to filter NMSs by source IPv4 address. The *acl-number* argument represents a basic ACL number in the range of 2000 to 2999. Only the NMSs with the IPv4 addresses permitted in the ACL can use the specified username to access the SNMP agent.

acl ipv6 *ipv6-acl-number*: Specifies a basic ACL to filter NMSs by source IPv6 address. The *ipv6-acl-number* argument represents a basic ACL number in the range of 2000 to 2999. Only the NMSs with the IPv6 addresses permitted in the ACL can use the specified username to access the SNMP agent.

local: Represents a local SNMP entity user.

engineid *engineid-string*: Specifies the SNMP engine ID as a hexadecimal string. The *engineid-string* argument must comprise an even number of hexadecimal characters, in the range of 10 to 64. All-zero and all-F strings are invalid.

Description

Use **snmp-agent usm-user v3** to create an SNMPv3 user in an SNMP group.

Use **undo snmp-agent usm-user v3** to delete an SNMPv3 user from an SNMP group.

You must create an SNMPv3 user for the agent and the NMS to use SNMPv3.

You must create an SNMP group before you assign an SNMP user to the group. Otherwise, the user cannot take effect after it is created. An SNMP group can contain multiple users. It defines SNMP objects accessible to the group of users in the MIB view and specifies whether to enable authentication and privacy functions. The authentication and encryption algorithms are defined when a user is created.

You can use the **snmp-agent calculate-password** command to obtain a hexadecimal ciphertext string for the *priv-password* argument in the **snmp-agent usm-user v3 cipher** command. To make the calculated cipher text password applicable to the **snmp-agent usm-user v3 cipher** command, make sure the same privacy protocol is specified for the two commands and the local engine ID specified in the **snmp-agent usm-user v3 cipher** command is consistent with the SNMP entity engine ID specified in the **snmp-agent calculate-password** command.

When you execute this command repeatedly to configure the same user (the usernames are the same, no limitation to other keywords and arguments), the last configuration takes effect.

For secrecy, both plaintext and ciphertext keys are saved in cipher text. Remember the username and the plaintext password when you create a user. A plaintext password is required when the NMS accesses the SNMP agent.

Related commands: **snmp-agent calculate-password**, **snmp-agent group**, and **snmp-agent usm-user { v1 | v2c }**.

Examples

Add the user **testUser** to the SNMPv3 group **testGroup**. Configure the security model as **authentication without privacy**, the authentication algorithm as **MD5**, and the plain-text key as **authkey**.

```
<Sysname> system-view
[Sysname] snmp-agent group v3 testGroup authentication
[Sysname] snmp-agent usm-user v3 testUser testGroup authentication-mode md5 authkey
```

- Set the SNMP version on the NMS to SNMPv3.
- Fill in the username **testUser**.
- Set the authentication algorithm to **MD5**.
- Set the authentication encrypted key to **authkey**.
- Establish a connection, and the NMS can access the MIB objects in the default view (ViewDefault) on the device.

Add the user **testUser** to the SNMPv3 group **testGroup**. Configure the security model as **authentication and privacy**, the authentication algorithm as MD5, the privacy algorithm as DES56, the plain-text authentication key as **authkey**, and the plain-text privacy key as **prikey**.

```
<Sysname> system-view
[Sysname] snmp-agent group v3 testGroup privacy
[Sysname] snmp-agent usm-user v3 testUser testGroup authentication-mode md5 authkey
privacy-mode des56 prikey
```

- Set the SNMP version on the NMS to SNMPv3.
- Fill in the username **testUser**.
- Set the authentication algorithm to **MD5**.
- Set the authentication key to **authkey**.
- Set the privacy algorithm to **DES**.
- Set the privacy key to **prikey**.
- Establish a connection, and the NMS can access the MIB objects in the default view (ViewDefault) on the device.

Add a user **testUser** to the SNMPv3 group **testGroup** with the **cipher** keyword specified. Configure the security model as **authentication and privacy**, the authentication algorithm as MD5, the privacy algorithm as DES56, the plain-text authentication key as **authkey**, and the plain-text privacy key as **prikey**.

```
<Sysname> system-view
[Sysname] snmp-agent group v3 testGroup privacy
[Sysname] snmp-agent calculate-password authkey mode md5 local-engineid
The secret key is: 09659EC5A9AE91BA189E5845E1DDE0CC
[Sysname] snmp-agent calculate-password prikey mode md5 local-engineid
The secret key is: 800D7F26E786C4BECE61BF01E0A22705
[Sysname] snmp-agent usm-user v3 testUser testGroup cipher authentication-mode md5
09659EC5A9AE91BA189E5845E1DDE0CC privacy-mode des56 800D7F26E786C4BECE61BF01E0A22705
```

- Set the SNMP version on the NMS to SNMPv3

- Fill in the username **testUser**,
- Set the authentication algorithm to **MD5**
- Set the authentication key to **authkey**
- Set the privacy algorithm to **DES**
- Set the privacy key to **prikey**
- Establish a connection, and the NMS can access the MIB objects in the default view(ViewDefault) on the device

RMON configuration commands

display rmon alarm

Syntax

display rmon alarm [*entry-number*] [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

entry-number: Specifies the index of an RMON alarm entry, in the range of 1 to 65535. If no entry is specified, the configuration of all alarm entries is 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 rmon alarm** to display the configuration of the specified RMON alarm entry or all RMON alarm entries.

Related commands: **rmon alarm**.

Examples

Display the configuration of all RMON alarm table entries.

```
<Sysname> display rmon alarm
```

```
AlarmEntry 1 owned by user1 is VALID.
```

```
Samples type           : absolute
Variable formula       : 1.3.6.1.2.1.16.1.1.1.4.1<etherStatsOctets.1>
Sampling interval      : 10(sec)
Rising threshold       : 50(linked with event 1)
Falling threshold      : 5(linked with event 2)
When startup enables   : risingOrFallingAlarm
Latest value           : 0
```

Table 23 Command output

Field	Description
AlarmEntry <i>entry-number</i> owned by <i>owner</i> is <i>status</i>	<p>Status of the alarm entry <i>entry-number</i> created by the owner is <i>status</i>:</p> <ul style="list-style-type: none"> • <i>entry-number</i>—Alarm entry, corresponding to the MIB node alarmIndex. • <i>owner</i>—Entry owner, corresponding to the MIB node alarmOwner. • <i>status</i>—Entry status, corresponding to the MIB node alarmStatus. <ul style="list-style-type: none"> ◦ VALID—The entry is valid. ◦ UNDERCREATION—The entry is invalid. <p>The display rmon command can display invalid entries, but the display current-configuration and display this commands do not display their settings.</p>
Samples type	Sampling type (the value can be absolute or delta), corresponding to the MIB node alarmSampleType.
Variable formula	Alarm variable, namely, the monitored MIB node, corresponding to the MIB node alarmVariable.
Sampling interval	Sampling interval, in seconds, corresponding to the MIB node alarmInterval.
Rising threshold	<p>Alarm rising threshold, corresponding to the MIB node alarmRisingThreshold.</p> <p>When the sampling value is greater than or equal to this threshold, a rising alarm is triggered.</p>
Falling threshold	<p>Alarm falling threshold, corresponding to the MIB node alarmFallingThreshold.</p> <p>When the sampling value is smaller than or equal to this threshold, a falling alarm is triggered.</p>
When startup enables	How an alarm can be triggered, corresponding to the MIB node alarmStartupAlarm.
Latest value	Last sampled value, corresponding to the MIB node alarmValue.

display rmon event

Syntax

```
display rmon event [ entry-number ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

entry-number: Specifies the index of an RMON event entry, in the range of 1 to 65535. If no entry is specified, the configuration of all event entries is 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 rmon event** to display the configuration of the specified RMON event entry or all RMON event entries.

Displayed information includes event index, event owner, event description, action triggered by the event (such as sending log or trap messages), and last time the event occurred (the elapsed time since system initialization/startup) in seconds.

Related commands: **rmon event**.

Examples

Display the configuration of the RMON event table.

```
<Sysname> display rmon event
```

```
EventEntry 1 owned by user1 is VALID.
```

```
    Description: null.
```

```
    Will cause log-trap when triggered, last triggered at 0days 00h:02m:27s.
```

Table 24 Command output

Field	Description
EventEntry	Event entry, corresponding to the MIB node eventIndex.
owned by	Event entry owner, corresponding to the MIB node eventOwner.
VALID	<p>Entry status:</p> <ul style="list-style-type: none">• VALID—The entry is valid.• UNDERCREATION—The entry is invalid. <p>The display rmon command can display invalid entries, but the display current-configuration and display this commands do not display their settings.</p> <p>Status value is stored in the MIB node eventStatus.</p>
Description	Event description, corresponding to the MIB node eventDescription.
cause log-trap when triggered	<p>Actions that the system will take when the event is triggered:</p> <ul style="list-style-type: none">• none—The system will take no action.• log—The system will log the event.• snmp-trap—The system will send a trap to the NMS.• log-and-trap—The system will log the event and send a trap to the NMS. <p>This field corresponds to the MIB node eventType.</p>
last triggered at	Time when the last event was triggered, corresponding to the MIB node eventLastTimeSent.

display rmon eventlog

Syntax

```
display rmon eventlog [ entry-number ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

entry-number: Specifies the index of an event entry, in the range of 1 to 65535.

|: 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 rmon eventlog** to display log information for the specified or all event entries.

If **entry-number** is not specified, log information for all event entries is displayed.

If you use the **rmon event** command to configure the system to log an event when the event is triggered, the event is recorded in the RMON log. You can use this command to display the details of the log table, which includes event index, current event state, time the event was logged (the elapsed time in seconds since system initialization/startup), and event description.

Examples

Display RMON log information for event entry 1.

```
<Sysname> display rmon eventlog 1
```

```
LogEntry 1 owned by null is VALID.
```

```
Generates eventLog 1.1 at 0day(s) 00h:00m:33s.
```

```
Description: The alarm formula defined in prialarmEntry 1,
```

```
uprise 80 with alarm value 85. Alarm sample type is absolute.
```

```
Generates eventLog 1.2 at 0day(s) 00h:42m:03s.
```

```
Description: The alarm formula defined in prialarmEntry 2,
```

```
less than(or =) 5 with alarm value 0. Alarm sample type is delta.
```

Table 25 Command output

Field	Description
LogEntry	Event entry, corresponding to the MIB node logIndex.
owned by	Event entry owner, corresponding to the MIB node eventOwner.
VALID	Entry status: <ul style="list-style-type: none">• VALID—The entry is valid.• UNDERCREATION—The entry is invalid. The display rmon command can display invalid entries, but the display current-configuration and display this commands do not display their settings. Status value is stored in the MIB node eventStatus.
Generates eventLog at	Time when the log was created (time passed since the device was booted), corresponding to the MIB node logTime.
Description	Log description, corresponding to the MIB node logDescription.

This example shows that event 1 generated two logs.

display rmon history

Syntax

```
display rmon history [ 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 *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 rmon history** to display RMON history control entry and history sampling information.

After you have created the history control entry on an interface, the system calculates the information of the interface periodically and saves the information to the etherHistoryEntry table. You can use this command to display the entries in this table.

To configure the number of history sampling records that can be displayed and the history sampling interval, use the **rmon history** command.

Related commands: **rmon history**.

Examples

Display RMON history control entry and history sampling information for interface GigabitEthernet 1/0/1.

```
<Sysname> display rmon history gigabitethernet 1/0/1
HistoryControlEntry 1 owned by null is VALID
  Samples interface      : GigabitEthernet1/0/1<ifIndex.1>
  Sampling interval      : 10(sec) with 5 buckets max
  Sampled values of record 1 :
    dropevents           : 0           , octets                : 3166
    packets               : 43          , broadcast packets     : 3
    multicast packets     : 6           , CRC alignment errors  : 0
    undersize packets     : 0           , oversize packets      : 0
    fragments             : 0           , jabbers               : 0
    collisions            : 0           , utilization            : 0
```

Sampled values of record 2 :

```
dropevents      : 0          , octets          : 834
packets         : 8          , broadcast packets : 1
multicast packets : 6        , CRC alignment errors : 0
undersize packets : 0        , oversize packets   : 0
fragments       : 0          , jabbers            : 0
collisions      : 0          , utilization         : 0
```

Sampled values of record 3 :

```
dropevents      : 0          , octets          : 1001
packets         : 9          , broadcast packets : 1
multicast packets : 7        , CRC alignment errors : 0
undersize packets : 0        , oversize packets   : 0
fragments       : 0          , jabbers            : 0
collisions      : 0          , utilization         : 0
```

Sampled values of record 4 :

```
dropevents      : 0          , octets          : 766
packets         : 7          , broadcast packets : 0
multicast packets : 6        , CRC alignment errors : 0
undersize packets : 0        , oversize packets   : 0
fragments       : 0          , jabbers            : 0
collisions      : 0          , utilization         : 0
```

Table 26 Command output

Field	Description
HistoryControlEntry	History control entry, which corresponds to MIB node etherHistoryIndex.
owned by	Entry owner, which corresponds to MIB node historyControlOwner.
VALID	<p>Entry status:</p> <ul style="list-style-type: none"> • VALID—The entry is valid. • UNDERCREATION—The entry is invalid. <p>The display rmon command can display invalid entries, but the display current-configuration and display this commands do not display their settings.</p> <p>Status value is stored in the MIB node historyControlStatus.</p>
Samples Interface	Sampled interface.
Sampling interval	Sampling period, in seconds, which corresponds to MIB node historyControlInterval. The system periodically samples the information of an interface.
buckets max	<p>Maximum number of history table entries that can be saved, corresponding to the MIB node historyControlBucketsGranted.</p> <p>If the specified value of the buckets argument exceeds the history table size supported by the device, the supported history table size is displayed.</p> <p>If the current number of the entries in the table has reached the maximum number, the system will delete the earliest entry to save the latest one.</p>
Sampled values of record <i>number</i>	The (<i>number</i>)th statistics recorded in the system cache. Statistics records are numbered according to the order of time they are saved into the cache.
dropevents	Dropped packets during the sampling period, corresponding to the MIB node etherHistoryDropEvents.

Field	Description
octets	Number of octets received during the sampling period, corresponding to the MIB node etherHistoryOctets.
packets	Number of packets received during the sampling period, corresponding to the MIB node etherHistoryPkts.
broadcastpackets	Number of broadcasts received during the sampling period, corresponding to the MIB node etherHistoryBroadcastPkts.
multicastpackets	Number of multicasts received during the sampling period, corresponding to the MIB node etherHistoryMulticastPkts.
CRC alignment errors	Number of packets received with CRC alignment errors during the sampling period, corresponding to the MIB node etherHistoryCRCAlignErrors.
undersize packets	Number of undersize packets received during the sampling period, corresponding to the MIB node etherHistoryUndersizePkts.
oversize packets	Number of oversize packets received during the sampling period, corresponding to the MIB node etherHistoryOversizePkts.
fragments	Number of fragments received during the sampling period, corresponding to the MIB node etherHistoryFragments.
jabbers	Number of jabbers received during the sampling period, corresponding to the MIB node etherHistoryJabbers.
collisions	Number of colliding packets received during the sampling period, corresponding to the MIB node etherHistoryCollisions.
utilization	Bandwidth utilization during the sampling period, corresponding to the MIB node etherHistoryUtilization.

display rmon prialarm

Syntax

```
display rmon prialarm [ entry-number ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

entry-number: Specifies the private alarm entry index in the range of 1 to 65535. If no entry is specified, the configuration of all private alarm entries is 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 rmon prialarm** to display the configuration of the specified private alarm entry or all private alarm entries.

Related commands: **rmon prialarm**.

Examples

Display the configuration of all private alarm entries.

```
<Sysname> display rmon prialarm
```

```
PrialarmEntry 1 owned by user1 is VALID.
```

```
Samples type           : absolute
Variable formula        : (.1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.1.16.1.1.1.5.1)
Description             : ifUtilization. GigabitEthernet1/0/1
Sampling interval       : 10(sec)
Rising threshold        : 80(linked with event 1)
Falling threshold       : 5(linked with event 2)
When startup enables    : risingOrFallingAlarm
This entry will exist   : forever
Latest value            : 85
```

Table 27 Command output

Field	Description
PrialarmEntry	Private alarm table entry.
owned by	Entry owner, user1 in this example.
VALID	Entry status: <ul style="list-style-type: none">• VALID—The entry is valid.• UNDERCREATION—The entry is invalid. The display rmon command can display invalid entries, but the display current-configuration and display this commands do not display their settings.
Samples type	Sampling type, whose value can be absolute or delta.
Description	Description of the private alarm entry.
Sampling interval	Sampling interval, in seconds. The system performs absolute sample or delta sample to sampling variables according to the sampling interval.
Rising threshold	Alarm rising threshold. An event is triggered when the sampled value is greater than or equal to this threshold.
Falling threshold	Alarm falling threshold. An event is triggered when the sampled value is less than or equal to this threshold.
linked with event	Event index associated with the prialarm.
When startup enables	How can an alarm be triggered.
This entry will exist	Lifetime of the entry, which can be forever or span the specified period.
Latest value	Count result of the last sample.

display rmon statistics

Syntax

display rmon statistics [*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 *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 rmon statistics** to display RMON statistics.

This command displays the interface statistics during the period from the time the statistics entry is created to the time the command is executed. The statistics are cleared when the device reboots.

Related commands: **rmon statistics**.

Examples

Display RMON statistics for GigabitEthernet 1/0/1.

```
<Sysname> display rmon statistics gigabitethernet 1/0/1
```

```
EtherStatsEntry 1 owned by null is VALID.
```

```
Interface : GigabitEthernet1/0/1<ifIndex.3>
```

```
etherStatsOctets          : 43393306 , etherStatsPkts          : 619825
```

```
etherStatsBroadcastPkts  : 503581 , etherStatsMulticastPkts : 44013
```

```
etherStatsUndersizePkts  : 0 , etherStatsOversizePkts  : 0
```

```
etherStatsFragments      : 0 , etherStatsJabbers      : 0
```

```
etherStatsCRCAlignErrors : 0 , etherStatsCollisions   : 0
```

```
etherStatsDropEvents (insufficient resources): 0
```

```
Packets received according to length:
```

```
64 : 0 , 65-127 : 0 , 128-255 : 0
```

```
256-511: 0 , 512-1023: 0 , 1024-1518: 0
```

Table 28 Command output

Field	Description
EtherStatsEntry	Entry of the statistics table, corresponding to MIB node etherStatsIndex.

Field	Description
VALID	<p>Entry status:</p> <ul style="list-style-type: none"> • VALID—The entry is valid. • UNDERCREATION—The entry is invalid. <p>The display rmon command can display invalid entries, but the display current-configuration and display this commands do not display their settings.</p> <p>Status value is stored in the MIB node etherStatsStatus.</p>
Interface	Interface on which statistics are gathered, which corresponds to the MIB node etherStatsDataSource.
etherStatsOctets	Number of octets received by the interface during the statistical period, corresponding to the MIB node etherStatsOctets.
etherStatsPkts	Number of packets received by the interface during the statistical period, corresponding to the MIB node etherStatsPkts.
etherStatsBroadcastPkts	Number of broadcast packets received by the interface during the statistical period, corresponding to the MIB node etherStatsBroadcastPkts.
etherStatsMulticastPkts	Number of multicast packets received by the interface during the statistical period, corresponding to the MIB node etherStatsMulticastPkts.
etherStatsUndersizePkts	Number of undersize packets received by the interface during the statistical period, corresponding to the MIB node etherStatsUndersizePkts.
etherStatsOversizePkts	Number of oversize packets received by the interface during the statistical period, corresponding to the MIB node etherStatsOversizePkts.
etherStatsFragments	Number of undersize packets with CRC errors received by the interface during the statistical period, corresponding to the MIB node etherStatsFragments.
etherStatsJabbers	Number of oversize packets with CRC errors received by the interface during the statistical period, corresponding to the MIB node etherStatsJabbers.
etherStatsCRCAlignErrors	Number of packets with CRC errors received on the interface during the statistical period, corresponding to the MIB node etherStatsCRCAlignErrors.
etherStatsCollisions	Number of collisions received on the interface during the statistical period, corresponding to the MIB node etherStatsCollisions.
etherStatsDropEvents	Total number of drop events received on the interface during the statistical period, corresponding to the MIB node etherStatsDropEvents.

Field	Description
Packets received according to length:	<p>Incoming-packet statistics by packet length for the statistical period:</p> <ul style="list-style-type: none"> • 64—Number of 64-byte packets. The value is stored in the MIB node <code>etherStatsPkts64Octets</code>. • 65-127—Number of 65- to 127-byte packets. The value is stored in the MIB node <code>etherStatsPkts65to127Octets</code>. • 128-255—Number of 128- to 255-byte packets. The value is stored in the MIB node <code>etherStatsPkts128to255Octets</code>. • 256-511—Number of 256- to 511-byte packets. The value is stored in the MIB node <code>etherStatsPkts256to511Octets</code>. • 512-1023—Number of 512- to 1023-byte packets. The value is stored in the MIB node <code>etherStatsPkts512to1023Octets</code>. • 1024-1518—Number of 1024- to 1518-byte packets. The value is stored in the MIB node <code>etherStatsPkts1024to1518Octets</code>.

rmon alarm

Syntax

rmon alarm *entry-number alarm-variable sampling-interval { absolute | delta } rising-threshold threshold-value1 event-entry1 falling-threshold threshold-value2 event-entry2 [owner text]*

undo rmon alarm *entry-number*

View

System view

Default level

2: System level

Parameters

entry-number: Specifies the alarm entry index in the range of 1 to 65535.

alarm-variable: Specifies the alarm variable, a string of 1 to 256 characters. It can be in dotted object identifier (OID) format (in the format of *entry.integer.instance* or *leaf node name.instance*, for example, 1.3.6.1.2.1.2.1.10.1), or a node name like `ifInOctets.1`. Only variables that can be parsed into INTEGER (INTEGER, Counter, Gauge, or Time Ticks) in the ASN.1 can be used for the *alarm-variable* argument, such as the instance of the leaf node (like `etherStatsOctets`, `etherStatsPkts`, `etherStatsBroadcastPkts`, and so on) of the `etherStatsEntry` entry, the instance of the leaf node (like `ifInOctets`, `ifInUcastPkts`, `ifInNUcastPkts`, and so on) of the `ifEntry` entry.

sampling-interval: Specifies the sampling interval in the range of 5 to 65535 seconds.

absolute: Sets the sampling type to **absolute**. In other words, the system obtains the value of the variable when the sampling time is reached.

delta: Sets the sampling type to **delta**. In other words, the system obtains the variation value of the variable during the sampling interval when the sampling time is reached.

rising-threshold threshold-value1 event-entry1: Sets the rising threshold, where the *threshold-value1* argument represents the rising threshold, in the range of -2147483648 to +2147483647, and the *event-entry1* argument represents the index of the event triggered when the rising threshold is reached.

The value range for the *event-entry1* argument is 0 to 65535. If 0 is specified, the alarm does not trigger any event.

falling-threshold *threshold-value2 event-entry2*: Sets the falling threshold, where the *threshold-value2* argument represents the falling threshold, in the range of -2147483648 to +2147483647 and the *event-entry2* argument represents the index of the event triggered when the falling threshold is reached. The value range for the *event-entry2* argument is 1 to 65535. If 0 is specified, the alarm does not trigger any event.

owner *text*: Specifies the owner of the entry, a case-sensitive string of 1 to 127 characters that can contain spaces.

Description

Use **rmon alarm** to create an entry in the RMON alarm table.

Use **undo rmon alarm** to remove an entry from the RMON alarm table.

You can create up to 60 alarm entries.

To make sure an alarm entry can take effect:

- Before creating an alarm entry, use the **rmon event** command to define the events to be referenced. Otherwise, the alarm entry cannot trigger events, even if it can be created.
- If the alarm variable is an instance of the leaf node of the Ethernet statistics table *etherStatsEntry* with the OID of 1.3.6.1.2.1.16.1.1.1, use the **rmon statistics** command to create a statistics entry on the monitored Ethernet interface. If the alarm variable is an instance of the leaf node of the history record table *etherHistoryEntry* with the OID of 1.3.6.1.2.1.16.2.2.1, use the **rmon history** command to create a history entry on the monitored Ethernet interface. Otherwise, the alarm entry cannot trigger events, even if it can be created.
- Make sure the alarm entry has different alarm variable (*alarm-variable*), sampling interval (*sampling-interval*), sampling type (**absolute** or **delta**), rising threshold (*threshold-value1*) and falling threshold (*threshold-value2*) than any existing alarm entry in the system.

When the alarm condition in an alarm entry occurs, its associated event is triggered to handle the alarm.

The system regularly samples the monitored alarm variables, compares the sampled values with the predefined thresholds, and does the following:

- If the rising threshold is reached, triggers the event specified by the *event-entry1* argument.
- If the falling threshold is reached, triggers the event specified by the *event-entry2* argument.

Related commands: **display rmon alarm**, **rmon event**, **rmon history**, and **rmon statistics**.

Examples

Add entry 1 in the alarm table and sample the node 1.3.6.1.2.1.16.1.1.1.4.1 at a sampling interval of 10 seconds in absolute sampling type. Trigger event 1 when the sampled value is greater than or equal to the rising threshold of 5000, and event 2 when the sampled value is less than or equal to the falling threshold of 5. Set the owner of the entry to be **user1**.

```
<Sysname> system-view
[Sysname] rmon event 1 log
[Sysname] rmon event 2 none
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 1
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.4.1 10 absolute rising-threshold 5000 1
falling-threshold 5 2 owner user1
```

1.3.6.1.2.1.16.1.1.1.4 is the OID of the leaf node etherStatsOctets. It represents the statistics of the received packets on the interface, in bytes. In the above example, you can use etherStatsOctets.1 to replace the parameter 1.3.6.1.2.1.16.1.1.1.4.1, where 1 indicates the serial number of the interface statistics entry. Therefore, if you execute the **rmon statistics 5** command, you can use etherStatsOctets.5 to replace the parameter.

This example enables the RMON agent to do the following:

- Samples and monitors interface GigabitEthernet 1/0/1.
- Obtains the incoming-packet count in its absolute value. If the total number of incoming bytes reaches 5000, the system logs the event. If the total number of incoming bytes is no more than 5, the system takes no action. To view the event log, use the **display rmon eventlog** command.

rmon event

Syntax

```
rmon event entry-number [ description string ] { log | log-trap log-trapcommunity | none | trap trap-community } [ owner text ]
```

```
undo rmon event entry-number
```

View

System view

Default level

2: System level

Parameters

entry-number: Specifies the event entry index in the range of 1 to 65535.

description *string*: Specifies the event description, a string of 1 to 127 characters.

log: Logs the event when it occurs.

log-trap *log-trapcommunity*: Specifies the log and trap events. The system performs both logging and trap sending when the event occurs. *log-trapcommunity* indicates the community name of the network management station that receives trap messages, a string of 1 to 127 characters.

none: Performs no action when the event occurs.

trap *trap-community*: Specifies the trap event. The system sends a trap with a community name when the event occurs. *trap-community* specifies the community name of the network management station that receives trap messages, a string of 1 to 127 characters.

owner *text*: Specifies the entry owner, a case-sensitive string of 1 to 127 characters that can contain spaces.

Description

Use **rmon event** to create an entry in the RMON event table.

Use **undo rmon event** to remove a specified entry from the RMON event table.

When creating an event entry, you can define the actions that the system takes when the event is triggered by its associated alarm in the alarm table. The system can log the event, send a trap, do both, or do neither based on your configuration.

An entry cannot be created if the values of the specified event description (**description string**), event type (**log**, **trap**, **logtrap** or **none**), and community name (*trap-community* or *log-trapcommunity*) to be identical to those of the existing event entry in the system.

Up to 60 event entries can be created.

Related commands: **display rmon event**, **rmon alarm**, and **rmon prialarm**.

Examples

```
# Create event 10 in the RMON event table.  
<Sysname> system-view  
[Sysname] rmon event 10 log owner user1
```

rmon history

Syntax

rmon history *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *text*]
undo rmon history *entry-number*

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

entry-number: Specifies the history control entry index in the range of 1 to 65535.

buckets *number*: Specifies the history table size for the entry, in the range of 1 to 65535.

interval *sampling-interval*: Specifies the sampling period in the range of 5 to 3600 seconds.

owner *text*: Specifies the owner of the entry, a case-sensitive string of 1 to 127 characters that can contain spaces.

Description

Use **rmon history** to create an entry in the RMON history control table.

Use **undo rmon history** to remove a specified entry from the RMON history control table.

After an entry is created, the system periodically samples the number of packets received/sent on the interface, and saves the statistics as an instance under the leaf node of the etherHistoryEntry table. The maximum number of statistics records can be saved for the entry is specified by **buckets** *number*. If the maximum number of the statistics records for the entry has been reached, the system deletes the earliest record for the latest one. The statistics include total number of received packets on the interface, total number of broadcast packets, total number of multicast packets in a sampling period, and so on.

You can successfully create a history control entry, even if the specified bucket size exceeds the history table size supported by the device. However, the effective bucket size will be the actual value supported by the device. To view the configuration result, use the **display rmon history** command.

You can configure multiple history control entries for one interface, but must make sure their entry numbers and sampling intervals are different.

The device supports up to 100 history control entries.

Related commands: **display rmon history**.

Examples

```
# Create RMON history control entry 1 for GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon history 1 buckets 10 interval 5 owner user1
```

rmon prialarm

Syntax

```
rmon prialarm entry-number prialarm-formula prialarm-des sampling-interval { absolute | changeratio | delta } rising-threshold threshold-value1 event-entry1 falling-threshold threshold-value2 event-entry2 entrytype { forever | cycle cycle-period } [ owner text ]
undo rmon prialarm entry-number
```

View

System view

Default level

2: System level

Parameters

entry-number: Specifies the index of a private alarm entry, in the range of 1 to 65535.

prialarm-formula: Specifies the private alarm variable formula, a string of 1 to 256 characters. The variables in the formula must be represented in OID format that starts with a dot (.), the formula (.1.3.6.1.2.1.2.1.10.1)*8 for example. You can customize the formula and perform the basic operations of addition, subtraction, multiplication, and division on these variables. The operations should yield a long integer. To prevent errors, make sure that the result of each calculating step falls into the value range for long integers.

prialarm-des: Specifies the private alarm entry description, a string of 1 to 127 characters.

sampling-interval: Specifies the sampling interval in the range of 10 to 65535 seconds.

absolute | **changeratio** | **delta**: Sets the sampling type to absolute, delta, or change ratio. Absolute sampling is to obtain the value of the variable when the sampling time is reached. Delta sampling is to obtain the variation value of the variable during the sampling interval when the sampling time is reached. Change ratio sampling is not supported at present.

rising-threshold threshold-value1 event-entry1: Sets the rising threshold, where the *threshold-value1* argument represents the rising threshold, in the range of -2147483648 to +2147483647, and the *event-entry1* argument represents the index of the event triggered when the rising threshold is reached. The value range for the *event-entry1* argument is 0 to 65535, where 0 means no corresponding event is triggered and no event action is taken when an alarm is triggered.

falling-threshold threshold-value2 event-entry2: Sets the falling threshold, where the *threshold-value2* argument represents the falling threshold, in the range of -2147483648 to +2147483647 and the *event-entry2* argument represents the index of the event triggered when the falling threshold is reached. The value range for the *event-entry2* argument is 1 to 65535.

forever: Indicates that the lifetime of the private alarm entry is infinite.

cycle cycle-period: Sets the lifetime period of the private alarm entry, in the range of 0 to 2147483647 seconds.

owner *text*: Specifies the entry owner, a case-sensitive string of 1 to 127 characters that can contain spaces.

Description

Use **rmon prialarm** to create an entry in the private alarm table of RMON.

Use **undo rmon prialarm** to remove a private alarm entry from the private alarm table of RMON.

Before creating an alarm entry, use the **rmon event** command to define the events to be referenced in the event table.

You cannot create an entry that has the same alarm variable formula (*prialarm-formula*), sampling type (**absolute** **changeratio** or **delta**), rising threshold (*threshold-value1*), and falling threshold (*threshold-value2*) as an existing private alarm entry.

You can create up to 50 private alarm entries.

The system handles private alarm entries as follows:

1. Samples the private alarm variables in the private alarm formula at the specified sampling interval.
2. Performs calculation on the sampled values with the formula.
3. Compares the calculation result with the predefined thresholds and does the following:
 - If the result is equal to or greater than the rising threshold, the system triggers the event specified by the *event-entry1* argument.
 - If the result is equal to or smaller than the falling threshold, the system triggers the event specified by the *event-entry2* argument.

Related commands: **display rmon prialarm**, **rmon event**, **rmon history**, and **rmon statistics**.

Examples

Monitor the ratio of the broadcast packets received on the interface by using the private alarm.

Calculate the private alarm variables with the (1.3.6.1.2.1.16.1.1.1.6.1 * 100 / 1.3.6.1.2.1.16.1.1.1.5.1) formula and sample the variables at 10-second intervals. (Broadcast packet ratio = total number of broadcast packets received on the interface / total number of packets received on the interface; the formula is customized by users.)

The rising threshold (80%) triggers event 1 to log the event. The falling threshold (5%) triggers event 2, but the event defines neither log nor trap action.

Set the lifetime of the entry to **forever** and owner to **user1**.

```
<Sysname> system-view
[Sysname] rmon event 1 log
[Sysname] rmon event 2 none
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 1
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] rmon prialarm 1 (.1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.1.16.1.1.1.5.1)
BroadcastPktsRatioOfGEth1/0/1 10 absolute rising-threshold 80 1 falling-threshold 5 2
entrytype forever owner user1
```

1.3.6.1.2.1.16.1.1.1.6.1 is the OID of the node etherStatsBroadcastPkts.1, and 1.3.6.1.2.1.16.1.1.1.5.1 is the OID of the node etherStatsPkts.1. 1 indicates the serial number of the interface statistics entry. Therefore, if you execute the **rmon statistics 5** command, you should use 1.3.6.1.2.1.16.1.1.1.6.5 and 1.3.6.1.2.1.16.1.1.1.5.5.

This example enables the RMON agent to do the following:

- Samples and monitors interface GigabitEthernet 1/0/1.
- If the portion of incoming broadcast packets in the total traffic crosses 80%, the system logs the event. If the portion is less than or equal to 5%, the system takes no action. To view the event log, use the **display rmon eventlog** command.

rmon statistics

Syntax

```
rmon statistics entry-number [ owner text ]
undo rmon statistics entry-number
```

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

entry-number: Specifies the statistics entry index in the range of 1 to 65535.

owner *text*: Specifies the owner of the entry, a string of case-sensitive 1 to 127 characters that can contain spaces.

Description

Use **rmon statistics** to create an entry in the RMON statistics table.

Use **undo rmon statistics** to remove a specified entry from the RMON statistics table.

You can create one statistics entry for each interface, and up to 100 statistics entries on the device.

Each RMON statistics table entry provides a set of cumulative traffic statistics collected up to the present time for an interface. Statistics include number of collisions, CRC alignment errors, number of undersize or oversize packets, number of broadcasts, number of multicasts, number of bytes received, and number of packets received. The statistics are cleared at a reboot.

To display the RMON statistics table, use the **display rmon statistics** command.

Examples

Create an entry with an index 20 and the owner **user1** in the RMON statistics table for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 20 owner user1
```

Port mirroring configuration commands

display mirroring-group

Syntax

```
display mirroring-group { group-id | all | local | remote-destination | remote-source } [ [ { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

2: System level

Parameters

group-id: Number of the mirroring group to be displayed, in the range of 1 to 4.

all: Displays all mirroring groups.

local: Displays local mirroring groups.

remote-destination: Displays remote destination groups.

remote-source: Displays remote source 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 mirroring-group** to display information about the specified mirroring groups, such as the types, status, and content of a mirroring group.

The output varies by mirroring group types and is sorted by mirroring group numbers.

Examples

Display information about all mirroring groups.

```
<Sysname> display mirroring-group all
mirroring-group 1:
  type: local
  status: active
  mirroring port:
    GigabitEthernet1/0/1  inbound
    GigabitEthernet1/0/2  both
  monitor port: GigabitEthernet1/0/3
mirroring-group 2:
```

```

type: remote-source
status: active
mirroring port:
    GigabitEthernet1/0/4  both
reflector port:
monitor egress port: GigabitEthernet1/0/8
remote-probe VLAN: 2
mirroring-group 3:
type: remote-destination
status: active
monitor port: GigabitEthernet1/0/7
remote-probe VLAN: 3

```

Table 29 Command output

Field	Description
mirroring-group	Number of the mirroring group
type	Type of the mirroring group, which can be local, remote-source, or remote-destination
status	Status of the mirroring group, which can be active or inactive
mirroring port	Source port
monitor egress port	Egress port of a remote source group
monitor port	Destination port

mirroring-group

Syntax

```

mirroring-group group-id { local | remote-destination | remote-source }
undo mirroring-group { group-id | all | local | remote-destination | remote-source }

```

View

System view

Default level

2: System level

Parameters

group-id: Specifies the number of the mirroring group to be created or removed, in the range of 1 to 4.

all: Removes all mirroring groups by using the **undo** command.

local: Creates a local mirroring group or removes all local mirroring groups with the **undo** command.

remote-destination: Creates a remote destination group or removes all remote destination groups with the **undo** command.

remote-source: Creates a remote source group or removes all remote source groups with the **undo** command.

Description

Use **mirroring-group** to create a mirroring group.

Use **undo mirroring-group** to remove the specified mirroring groups.

To mirror packets from a port to another port on the same device, create a local mirroring group.

To mirror packets from a port (a source port) on the current device to another port (the monitor port) either on the same device or on a different device, create remote mirroring groups. When doing that, create the remote source group on the device where the source port is located and create the remote destination group on the device where the monitor port is located.

By default, no mirroring group exists on a device.

Related commands: **sampler**.

Examples

```
# Create a local mirroring group numbered 1.
```

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

```
[Sysname] mirroring-group 1 local
```

mirroring-group mirroring-port

Syntax

mirroring-group *group-id* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** }

undo mirroring-group *group-id* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** }

View

System view

Default level

2: System level

Parameters

group-id: Number of a local or remote source group, in the range of 1 to 4. The mirroring group specified by the *group-id* argument must already exist.

mirroring-port-list: A list of source ports/port ranges to be assigned to or removed from the mirroring group specified by *group-id*. You can specify up to eight single ports, port ranges, or combinations of both for the list. A single port takes the form of *interface-type interface-number*. A port range takes the form *interface-type interface-number to interface-type interface-number*, where the end port number must be greater than the start port number. For example, you may specify up to eight combinations of single ports and port ranges for the list like this: **gigabitethernet 1/0/1 gigabitethernet 1/0/3 gigabitethernet 1/0/5 gigabitethernet 2/0/2 to gigabitethernet 2/0/10 gigabitethernet 3/0/1 gigabitethernet 3/0/4 gigabitethernet 3/0/6 to gigabitethernet 3/0/10 gigabitethernet 3/0/12**.

both: Mirrors both inbound and outbound packets on the specified ports.

inbound: Mirrors only inbound packets on the specified ports.

outbound: Mirrors only outbound packets on the specified ports.

Description

Use **mirroring-group mirroring-port** to assign ports to a local or remote source group as source ports.

Use **undo mirroring-group mirroring-port** to remove source ports from the mirroring group.

By default, no source port is configured for any mirroring group.

You cannot configure source ports for a remote destination group.

When removing a source port from a mirroring group, make sure the traffic direction you specified in the **undo mirroring-group mirroring-port** command matches the actual monitored direction specified earlier in the **mirroring-group mirroring-port** command.

Related commands: **mirroring-group**.

Examples

Create local mirroring group 1, configure GigabitEthernet 1/0/1 as a source port of the mirroring group, and specify that the mirroring group monitor the bidirectional traffic of the port.

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

```
[Sysname] mirroring-group 1 local
```

```
[Sysname] mirroring-group 1 mirroring-port GigabitEthernet 1/0/1 both
```

Create remote source group 2, configure GigabitEthernet 1/0/2 as a source port of the mirroring group, and specify that the mirroring group monitor the bidirectional traffic of the port.

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

```
[Sysname] mirroring-group 2 remote-source
```

```
[Sysname] mirroring-group 2 mirroring-port GigabitEthernet 1/0/2 both
```

mirroring-group monitor-egress

Syntax

In system view:

mirroring-group *group-id* **monitor-egress** *monitor-egress-port*

undo mirroring-group *group-id* **monitor-egress** *monitor-egress-port*

In interface view:

mirroring-group *group-id* **monitor-egress**

undo mirroring-group *group-id* **monitor-egress**

View

System view, interface view

Default level

2: System level

Parameters

group-id: Number of a remote source group, in the range of 1 to 4. The mirroring group specified by *group-id* must already exist.

monitor-egress-port: Port to be configured as the egress port. It takes the form of *interface-type interface-number*, where *interface-type* specifies the port type and *interface-number* specifies the port number.

Description

Use **mirroring-group monitor-egress** to configure a port as the egress port of a remote source group.

Use **undo mirroring-group monitor-egress** to remove the egress port of the mirroring group.

By default, no egress port is configured for a mirroring group.

You can configure an egress port only for a remote source group, not for other types of mirroring groups.

Related commands: **mirroring-group**.

Examples

Create remote source group 1, and configure port GigabitEthernet 1/0/1 as its egress port in system view.

```
<Sysname> system-view
[Sysname] mirroring-group 1 remote-source
[Sysname] mirroring-group 1 monitor-egress GigabitEthernet 1/0/1
```

Create remote source group 2, and configure port GigabitEthernet 1/0/2 as its egress port in interface view.

```
<Sysname> system-view
[Sysname] mirroring-group 2 remote-source
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] mirroring-group 2 monitor-egress
```

mirroring-group monitor-port

Syntax

mirroring-group *group-id* **monitor-port** *monitor-port-id*
undo mirroring-group *group-id* **monitor-port** *monitor-port-id*

View

System view

Default level

2: System level

Parameters

group-id: Number of a local or remote destination group, in the range of 1 to 4. The mirroring group specified by *group-id* must already exist.

monitor-port-id: Port to be assigned to the specified mirroring group as the monitor port. The argument takes the form of *interface-type interface-number*, where *interface-type* specifies the port type and *interface-number* specifies the port number.

Description

Use **mirroring-group monitor-port** to assign a port to a local or remote destination group as the monitor port.

Use **undo mirroring-group monitor-port** to remove the monitor port from the local or remote destination group.

By default, no monitor port is configured for a mirroring group.

You cannot configure a monitor port for a remote source group.

You cannot assign a source port in an existing mirroring group to another mirroring group as the monitor port.

Related commands: **mirroring-group**.

Examples

```
# Create local mirroring group 1, and configure port GigabitEthernet 1/0/1 as its monitor port.
<Sysname> system-view
[Sysname] mirroring-group 1 local
[Sysname] mirroring-group 1 monitor-port GigabitEthernet 1/0/1

# Create remote destination group 2, and configure port GigabitEthernet 1/0/2 as its monitor port.
<Sysname> system-view
[Sysname] mirroring-group 2 remote-destination
[Sysname] mirroring-group 2 monitor-port GigabitEthernet 1/0/2
```

mirroring-group reflector-port

Syntax

In system view:

```
mirroring-group group-id reflector-port reflector-port
undo mirroring-group group-id reflector-port reflector-port
```

In interface view:

```
mirroring-group group-id reflector-port
undo mirroring-group group-id reflector-port
```

View

System view, interface view

Default level

2: System level

Parameters

group-id: Number of a remote source group, in the range of 1 to 4. The mirroring group specified by *group-id* must already exist.

reflector-port: Port to be configured as the reflector port in the specified mirroring group. The argument takes the form of *interface-type interface-number*, where *interface-type* specifies the port type and *interface-number* specifies the port number.

Description

Use **mirroring-group reflector-port** to configure the reflector port in a remote source group.

Use **undo mirroring-group reflector-port** to remove the reflector port of the remote source group.

By default, no reflector port is configured for a mirroring group, and a port does not serve as the reflector port of any mirroring group.

You can configure a reflector port for a remote source group only, not for other types of mirroring groups.

Related commands: **mirroring-group**.

Examples

```
# Create remote source group 1, and configure port GigabitEthernet 1/0/1 as its reflector port in system view.
<Sysname> system-view
[Sysname] mirroring-group 1 remote-source
```



```
[Sysname] mirroring-group 1 reflector-port GigabitEthernet 1/0/1
# Create remote source group 2, and configure port GigabitEthernet 1/0/2 as its reflector port in
interface view.
<Sysname> system-view
[Sysname] mirroring-group 2 remote-source
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] mirroring-group 2 reflector-port
```

mirroring-group remote-probe vlan

Syntax

```
mirroring-group group-id remote-probe vlan rprobe-vlan-id
undo mirroring-group group-id remote-probe vlan rprobe-vlan-id
```

View

System view

Default level

2: System level

Parameters

group-id: Number of a remote source or destination mirroring group, in the range of 1 to 4. The mirroring group specified by *group-id* must already exist.

rprobe-vlan-id: ID of the VLAN to be configured as the remote probe VLAN. This VLAN must be a static VLAN that already exists.

Description

Use **mirroring-group remote-probe vlan** to specify a VLAN as the remote probe VLAN for a remote source or destination mirroring group.

Use **undo mirroring-group remote-probe vlan** to remove the remote probe VLAN from the remote source or destination mirroring group.

By default, no remote probe VLAN is configured for a mirroring group.

For a remote source or destination mirroring group, you must configure and can configure only one remote probe VLAN to carry mirrored packets. You cannot configure the remote probe VLAN for a local mirroring group.

Only a static VLAN that already exists can be configured as a remote probe VLAN. A VLAN can serve as the remote probe VLAN of only one mirroring group.

To delete a VLAN that is configured as a remote probe VLAN, remove the remote probe VLAN configuration first.

Related commands: **mirroring-group**.

Examples

```
# Create remote source group 1, and configure VLAN 10 as its remote probe VLAN.
<Sysname> system-view
[Sysname] mirroring-group 1 remote-source
[Sysname] mirroring-group 1 remote-probe vlan 10

# Create remote destination group 2, and configure VLAN 20 as its remote probe VLAN.
```

```
<Sysname> system-view
[Sysname] mirroring-group 2 remote-destination
[Sysname] mirroring-group 2 remote-probe vlan 20
```

mirroring-port

Syntax

```
[ mirroring-group group-id ] mirroring-port { inbound | outbound | both }
undo [ mirroring-group group-id ] mirroring-port { inbound | outbound | both }
```

View

Interface view

Default level

2: System level

Parameters

mirroring-group group-id: Specifies a local or remote source group by its number, which ranges from 1 to 4 and defaults to 1. The mirroring group specified by *group-id* must already exist.

both: Mirrors both inbound and outbound packets on the current port.

inbound: Mirrors only inbound packets on the current port.

outbound: Mirrors only outbound packets on the current port.

Description

Use **mirroring-port** to assign the current port to a local or remote source group as a source port.

Use **undo mirroring-port** to remove the current port from the mirroring group.

By default, a port does not serve as a source port for any mirroring group.

You cannot configure source ports for a remote destination group.

When removing a source port from a mirroring group, make sure the traffic direction you specified in the **undo mirroring-group** command matches the actual monitored direction of the port specified earlier in the **mirroring-port** command.

Examples

Create local mirroring group 1, configure GigabitEthernet 1/0/1 as a source port of the mirroring group, and specify that the mirroring group monitor the bidirectional traffic of the port.

```
<Sysname> system-view
[Sysname] mirroring-group 1 local
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mirroring-group 1 mirroring-port both
```

Create remote source group 2, configure GigabitEthernet 1/0/2 as a source port of the mirroring group, and specify that the mirroring group monitor the bidirectional traffic of the port.

```
<Sysname> system-view
[Sysname] mirroring-group 2 remote-source
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] mirroring-group 2 mirroring-port both
```

monitor-port

Syntax

```
[ mirroring-group group-id ] monitor-port  
undo [ mirroring-group group-id ] monitor-port
```

View

Interface view

Default level

2: System level

Parameters

mirroring-group *group-id*: Specifies a local or remote destination group by its number, which ranges from 1 to 4 and defaults to 1. The mirroring group specified by *group-id* must already exist.

Description

Use **monitor-port** to assign the current port to a local or remote destination group as the monitor port.

Use **undo monitor-port** to remove the current port from the mirroring group.

By default, a port does not serve any mirroring group as the monitor port.

You cannot configure a monitor port for a remote source group.

You cannot configure a source port of an existing mirroring group as a monitor port.

Related commands: **mirroring-group**.

Examples

Create local mirroring group 1, and configure GigabitEthernet 1/0/1 as its monitor port.

```
<Sysname> system-view  
[Sysname] mirroring-group 1 local  
[Sysname] interface GigabitEthernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] monitor-port
```

Create remote destination group 2, and configure GigabitEthernet 1/0/2 as its monitor port.

```
<Sysname> system-view  
[Sysname] mirroring-group 2 remote-destination  
[Sysname] interface GigabitEthernet 1/0/2  
[Sysname-GigabitEthernet1/0/2] monitor-port
```

Traffic mirroring configuration commands

The traffic mirroring and remote traffic mirroring functions on the switch are implemented through the cooperation of a QoS policy and remote port mirroring. For the configuration commands about a QoS policy, see *ACL and QoS Command Reference*.

mirror-to

Syntax

```
mirror-to { cpu | interface interface-type interface-number }  
undo mirror-to { cpu | interface interface-type interface-number }
```

View

Traffic behavior view

Default level

2: System level

Parameters

cpu: Mirrors traffic to the CPU, which is the CPU of the device where ports with traffic mirroring configured resides.

interface *interface-type interface-number*: Mirrors traffic to a port specified by its type and number.

Description

Use **mirror-to** to configure traffic mirroring for a traffic behavior.

Use **undo mirror-to** to remove traffic mirroring configuration.

By default, traffic mirroring is not configured for a traffic behavior.

You can configure the action of mirroring traffic to a port multiple times for a traffic behavior. Traffic can only be mirrored to the CPU or a port in a traffic behavior.

Examples

Create traffic behavior 1 and configure the action of mirroring traffic to the CPU for the traffic behavior.

```
<Sysname> system-view  
[Sysname] traffic behavior 1  
[Sysname-behavior-1] mirror-to cpu
```

Create traffic behavior 1 and configure the action of mirroring traffic to port GigabitEthernet 1/0/1 for the traffic behavior.

```
<Sysname> system-view  
[Sysname] traffic behavior 1  
[Sysname-behavior-1] mirror-to interface GigabitEthernet 1/0/1
```

NQA configuration commands

NQA client configuration commands

advantage-factor

Syntax

advantage-factor *factor*
undo advantage-factor

View

Voice operation view

Default level

2: System level

Parameters

factor: Specifies the advantage factor, used to count Mean Opinion Scores (MOS) and Calculated Planning Impairment Factor (ICPIF) values. The value is in the range of 0 to 20.

Description

Use **advantage-factor** to configure the advantage factor that is used to count MOS and ICPIF values.

Use **undo advantage-factor** to restore the default.

By default, the advantage factor is 0.

The evaluation of voice quality depends on users' tolerance for voice quality, and this factor should be taken into consideration. For users with higher tolerance for voice quality, use the **advantage-factor** command to configure the advantage factor. When the system calculates the ICPIF value, this advantage factor is subtracted to modify ICPIF and MOS values and both the objective and subjective factors are considered when you evaluate voice quality.

Examples

```
# Configure the advantage factor for a voice test as 10.  
<Sysname> system-view  
[Sysname] nqa entry admin test  
[Sysname-nqa-admin-test] type voice  
[Sysname-nqa-admin-test-voice] advantage-factor 10
```

codec-type

Syntax

codec-type { **g711a** | **g711u** | **g729a** }
undo codec-type

View

Voice operation view

Default level

2: System level

Parameters

g711a: Specifies a G.711 A-law codec type.

g711u: Specifies a G.711 μ -law codec type

g729a: Specifies a G.729 A-law codec type.

Description

Use **codec-type** to configure the codec type for a voice test.

Use **undo codec-type** to restore the default.

By default, the codec type for a voice test is G.711 A-law.

Examples

Configure the codec type for a voice test as **g729a**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type voice
[Sysname-nqa-admin-test-voice] codec-type g729a
```

data-fill

Syntax

data-fill *string*

undo data-fill

View

ICMP echo, UDP echo, UDP jitter, voice operation view

Default level

2: System level

Parameters

string: Specifies a case-sensitive string of 1 to 200 characters.

Description

Use **data-fill** to configure the string to be filled in the data field of a probe packet.

Use **undo data-fill** to restore the default.

By default, the string is the hexadecimal number 00010203040506070809.

- If the data field length is smaller than the string length, only the first part of the string is filled. For example, if you configure the string as **abcd** and the data field size as 3 bytes, **abc** is filled.
- If the data field length is greater than the string length, the system fills the data field with the string cyclically until the data field is full. For example, if you configure the string as **abcd** and the data field size as 6 bytes, **abcdab** is filled.

How the string is filled varies with test types:

- For ICMP echo tests, the string fills the whole data field of ICMP echo requests.
- For UDP echo tests, the first five bytes of the data field of a UDP packet are for special purpose, so the string fills the remaining part of data field.
- For UDP jitter tests, the first 68 bytes of the data field of a UDP packet are for special purpose, so the string fills the remaining part of the data field.
- For voice tests, the first 16 bytes of the data field of a UDP packet are for special purpose, so the string fills the remaining part of the data field.

Examples

Configure string **abcd** to be filled in the data field of an ICMP echo request.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] data-fill abcd
```

data-size

Syntax

data-size *size*

undo data-size

View

ICMP echo, UDP echo, UDP jitter, voice operation view

Default level

2: System level

Parameters

size: Specifies the size of the data field in a probe packet in bytes. The value is in the range of 20 to 8100 for probe packets of ICMP echo or UDP echo tests, 68 to 8100 for probe packets of UDP jitter tests, and 16 to 1500 for probe packets of voice tests.

Description

Use **data-size** to configure the size of the data field in each ICMP echo request of the ICMP echo tests or in each UDP packet of UDP echo, UDP jitter, or voice tests.

Use **undo data-size** to restore the default.

Table 30 Default values of the size of a probe packet

Operation	Codec type	Default value (in bytes)
ICMP echo	N/A	100
UDP echo	N/A	100
UDP jitter	N/A	100
Voice	G.711 A-law	172
Voice	G.711 μ -law	172
Voice	G.729 A-law	32

Examples

```
# Configure the size of the data field in an ICMP echo request as 80 bytes.
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] data-size 80
```

description (any NQA operation view)

Syntax

description *text*
undo description

View

Any NQA operation view

Default level

2: System level

Parameters

text: Specifies a case-sensitive string of 1 to 200 characters, used to describe a test group.

Description

Use **description** to give a brief description of a test group, usually, the test type or test purpose of a test group.

Use **undo description** to remove the configured description information.

By default, no descriptive string is available for a test group.

Examples

```
# Configure the descriptive string for a test group as icmp-probe.
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] description icmp-probe
```

destination ip

Syntax

destination ip *ip-address*
undo destination ip

View

DLSw, FTP, DNS, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice operation view

Default level

2: System level

Parameters

ip-address: Specifies the destination IP address of a test operation.

Description

Use **destination ip** to configure a destination IP address for a test operation.

Use **undo destination ip** to remove the configured destination IP address.

By default, no destination IP address is configured for a test operation.

Examples

Configure the destination IP address of an ICMP echo test operation as 10.1.1.1.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] destination ip 10.1.1.1
```

destination port

Syntax

destination port *port-number*

undo destination port

View

TCP, UDP echo, UDP jitter, voice operation view

Default level

2: System level

Parameters

port-number: Specifies the destination port number of a test operation, in the range of 1 to 65535.

Description

Use **destination port** to configure a destination port number for a test operation.

Use **undo destination port** to remove the configured destination port number.

By default, no destination port number is configured for a test operation.

Do not perform a UDP jitter test and a voice test on ports from 1 to 1023 (known ports). Otherwise, the NQA test fails or the corresponding services of this port are unavailable.

Examples

Configure the destination port number of a test operation as 9000.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-echo
[Sysname-nqa-admin-test-udp-echo] destination port 9000
```

display nqa history

Syntax

display nqa history [*admin-name operation-tag*] [[{ **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

admin-name operation-tag: Displays history records of an NQA test group. If these two arguments are not specified, history records of all test groups are displayed. **admin-name** represents the name of the NQA test group administrator who creates the NQA operation. It is a case-insensitive string of 1 to 32 characters. **operation-tag** represents the test operation tag. It is a case-insensitive string of 1 to 32 characters.

|: 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 nqa history** to display history records of the specified or all NQA test groups.

The **display nqa history** command cannot show you the results of voice tests and UDP jitter tests. To know the result of a voice test or a UDP jitter test, use the **display nqa result** command to view the probe results of the latest NQA test, or use the **display nqa statistics** command to view the statistics of NQA tests.

Examples

Display the history records of the NQA test group in which the administrator name is **administrator**, and the operation tag is **test**.

```
<Sysname> display nqa history administrator test
NQA entry (admin administrator, tag test) history record(s):
  Index      Response      Status      Time
  10         329           Succeeded   2011-01-23 20:54:26.5
   9         344           Succeeded   2011-01-23 20:54:26.2
   8         328           Succeeded   2011-01-23 20:54:25.8
   7         328           Succeeded   2011-01-23 20:54:25.5
   6         328           Succeeded   2011-01-23 20:54:25.1
   5         328           Succeeded   2011-01-23 20:54:24.8
   4         328           Succeeded   2011-01-23 20:54:24.5
   3         328           Succeeded   2011-01-23 20:54:24.1
   2         328           Succeeded   2011-01-23 20:54:23.8
   1         328           Succeeded   2011-01-23 20:54:23.4
```

Table 31 Command output

Field	Description
Index	History record number
Response	Round-trip delay of a test packet in the case of a successful test, timeout time in the case of timeout, or 0 in the case that a test cannot be completed (in milliseconds)

Field	Description
Status	Status value of test results, which can be one of the following values: <ul style="list-style-type: none"> • Succeeded • Unknown error • Internal error • Timeout
Time	Time when the test is completed

display nqa reaction counters

Syntax

```
display nqa reaction counters [ admin-name operation-tag [ item-number ] ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

admin-name operation-tag: Displays current monitoring results of reaction entries in a test group. If these two arguments are not specified, monitoring results of all reaction entries of all test groups are displayed. *admin-name* represents the name of the NQA test group administrator who creates the NQA operation. It is a case-insensitive string of 1 to 32 characters. *operation-tag* represents the test operation tag. It is a case-insensitive string of 1 to 32 characters.

item-number: Displays current monitoring results of a specific reaction entry. If this argument is not provided, results of all reaction entries are displayed. *item-number* represents the reaction entry ID, in the range of 1 to 10.

|: 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 nqa reaction counters** to display the current monitoring results of reaction entries.

If the threshold type is average value, or the monitored element is ICMP or MOS in a voice test, the monitoring results are invalid.

The monitoring results are accumulated since the test group starts and are not cleared after the test completes.

Examples

```
# Display the monitoring results of all reaction entries in an ICMP echo test group, in which the administrator name is admin, and the operation tag is test.
```

```
<Sysname> display nqa reaction counters admin test
NQA entry (admin admin, tag test) reaction counters:
  Index  Checked Element  Threshold Type  Checked Num  Over-threshold Num
  1      probe-duration  accumulate     12           4
  2      probe-duration  average        -            -
  3      probe-duration  consecutive    160          56
  4      probe-fail      accumulate     12           0
  5      probe-fail      consecutive    162          2
```

Table 32 Command output

Field	Description
Index	ID of a reaction entry
Checked Element	Monitored element
Threshold Type	Threshold type
Checked Num	Number of targets that have been monitored for data collection
Over-threshold Num	Number of threshold violations

Table 33 Description on the threshold monitoring fields of the display nqa reaction counters command

Monitored element	Threshold type	Collect data in	Checked Num	Over-threshold Num
probe-duration	accumulate	Probes since the group starts	Number of finished probes since the test group starts	Number of probes of which the duration exceeds the threshold since the test group starts
	average	N/A	N/A	N/A
	consecutive	Probes since the test group starts	Number of finished probes since the test group starts	Number of probes of which the duration exceeds the threshold since the test group starts
probe-fail	accumulate	Probes since the test group starts	Number of finished probes since the test group starts	Number of probe failures since the test group starts
	consecutive	Probes since the test group starts	Number of finished probes since the test group starts	Number of probe failures since the test group starts
RTT	accumulate	Packets sent since the test group starts	Number of packets sent since the test group starts	Number of packets of which the round-trip time exceeds the threshold since the test group starts
	average	N/A	N/A	N/A

Monitored element	Threshold type	Collect data in	Checked Num	Over-threshold Num
jitter-DS/jitter-SD	accumulate	Packets sent since the test group starts	Number of packets sent since the test group starts	Number of packets of which the one-way delay jitter exceeds the threshold since the test group starts
	average	N/A	N/A	N/A
OWD-DS/OWD-SD	N/A	Packets sent since the test group starts	Number of packets sent since the test group starts	Number of packets of which the one-way delay exceeds the threshold since the test group starts
packet-loss	accumulate	Packets sent since the test group starts	Number of packets sent since the test group starts	Total packet loss since the test group starts
ICPIF	N/A	N/A	N/A	N/A
MOS	N/A	N/A	N/A	N/A

display nqa result

Syntax

```
display nqa result [ admin-name operation-tag ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

admin-name operation-tag: Displays results of the last test of a test group. If these two arguments are not specified, results of the last tests of all test groups are displayed. *admin-name* represents the name of the NQA test group administrator who creates the NQA operation, and it is a case-insensitive string of 1 to 32 characters. *operation-tag* represents the test operation tag, and it is a case-insensitive string of 1 to 32 characters.

|: 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 nqa result** to display results of the last NQA test.

Examples

```
# Display the results of the last UDP jitter test.
```

```

<Sysname> display nqa result admin test
NQA entry (admin admin, tag test) test results:
  Destination IP address: 192.168.1.42
    Send operation times: 10          Receive response times: 10
    Min/Max/Average round trip time: 15/46/26
    Square-Sum of round trip time: 8103
    Last succeeded probe time: 2011-01-23 10:56:38.7
Extended results:
  Packet loss in test: 0%
  Failures due to timeout: 0
  Failures due to disconnect: 0
  Failures due to no connection: 0
  Failures due to sequence error: 0
  Failures due to internal error: 0
  Failures due to other errors: 0
  Packet(s) arrived late: 0
UDP-jitter results:
  RTT number: 10
    Min positive SD: 8                Min positive DS: 8
    Max positive SD: 18               Max positive DS: 8
    Positive SD number: 5             Positive DS number: 2
    Positive SD sum: 75                Positive DS sum: 32
    Positive SD average: 15           Positive DS average: 16
    Positive SD square sum: 1189       Positive DS square sum: 640
    Min negative SD: 8                Min negative DS: 1
    Max negative SD: 24               Max negative DS: 30
    Negative SD number: 4             Negative DS number: 7
    Negative SD sum: 56                Negative DS sum: 99
    Negative SD average: 14           Negative DS average: 14
    Negative SD square sum: 946        Negative DS square sum: 1495
One way results:
  Max SD delay: 22                    Max DS delay: 23
  Min SD delay: 7                     Min DS delay: 7
  Number of SD delay: 10              Number of DS delay: 10
  Sum of SD delay: 125                Sum of DS delay: 132
  Square sum of SD delay: 1805         Square sum of DS delay: 1988
  SD lost packet(s): 0                DS lost packet(s): 0
  Lost packet(s) for unknown reason: 0

```

Display the results of the last voice test.

```

<Sysname> display nqa result admin test
NQA entry (admin admin, tag test) test results:
  Destination IP address: 192.168.1.42
    Send operation times: 1000        Receive response times: 0
    Min/Max/Average round trip time: 0/0/0
    Square-Sum of round trip time: 0
    Last succeeded probe time: 0-00-00 00:00:00.0
Extended results:
  Packet loss in test: 100%

```

```

Failures due to timeout: 1000
Failures due to disconnect: 0
Failures due to no connection: 0
Failures due to sequence error: 0
Failures due to internal error: 0
Failures due to other errors: 0
Packet(s) arrived late: 0
Voice results:
RTT number: 0
Min positive SD: 0           Min positive DS: 0
Max positive SD: 0           Max positive DS: 0
Positive SD number: 0        Positive DS number: 0
Positive SD sum: 0           Positive DS sum: 0
Positive SD average: 0       Positive DS average: 0
Positive SD square sum: 0    Positive DS square sum: 0
Min negative SD: 0           Min negative DS: 0
Max negative SD: 0           Max negative DS: 0
Negative SD number: 0        Negative DS number: 0
Negative SD sum: 0           Negative DS sum: 0
Negative SD average: 0       Negative DS average: 0
Negative SD square sum: 0    Negative DS square sum: 0
One way results:
Max SD delay: 0             Max DS delay: 0
Min SD delay: 0             Min DS delay: 0
Number of SD delay: 0       Number of DS delay: 0
Sum of SD delay: 0          Sum of DS delay: 0
Square sum of SD delay: 0   Square sum of DS delay: 0
SD lost packet(s): 0        DS lost packet(s): 0
Lost packet(s) for unknown reason: 1000
Voice scores:
MOS value: 0.99             ICPIF value: 87

```

Table 34 Command output

Field	Description
Destination IP address	IP address of the destination
Send operation times	Number of probe packets sent
Receive response times	Number of response packets received
Min/Max/Average round trip time	Minimum/maximum/average round-trip time in milliseconds
Square-Sum of round trip time	Square sum of round-trip time
Last succeeded probe time	Time when the last successful probe was finished
Packet loss in test	Average packet loss ratio
Failures due to timeout	Number of timeout occurrences in a test
Failures due to disconnect	Number of disconnections by the peer
Failures due to no connection	Number of failures to connect with the peer
Failures due to sequence error	Number of failures due to out-of-sequence packets

Field	Description
Failures due to internal error	Number of failures due to internal errors
Failures due to other errors	Failures due to other errors
Packet(s) arrived late	Number of packets that arrived late
UDP-jitter results	UDP jitter test results, available only in UDP jitter tests
Voice results	Voice test results, available only in voice tests
RTT number	Number of response packets received
Min positive SD	Minimum positive delay jitters from source to destination
Min positive DS	Minimum positive delay jitters from destination to source
Max positive SD	Maximum positive delay jitters from source to destination
Max positive DS	Maximum positive delay jitters from destination to source
Positive SD number	Number of positive delay jitters from source to destination
Positive DS number	Number of positive delay jitters from destination to source
Positive SD sum	Sum of positive delay jitter from source to destination
Positive DS sum	Sum of positive delay jitters from destination to source
Positive SD average	Average of positive delay jitter from source to destination
Positive DS average	Average of positive delay jitter from destination to source
Positive SD square sum	Square sum of positive delay jitters from source to destination
Positive DS square sum	Square sum of positive delay jitters from destination to source
Min negative SD	Minimum absolute value among negative delay jitters from source to destination
Min negative DS	Minimum absolute value among negative delay jitters from destination to source
Max negative SD	Maximum absolute value among negative delay jitters from source to destination
Max negative DS	Maximum absolute value among negative delay jitters from destination to source
Negative SD number	Number of negative delay jitters from source to destination
Negative DS number	Number of negative delay jitters from destination to source
Negative SD sum	Sum of absolute values of negative delay jitters from source to destination
Negative DS sum	Sum of absolute values of negative delay jitters from destination to source
Negative SD average	Average absolute value of negative delay jitters from source to destination
Negative DS average	Average absolute value of negative delay jitters from destination to source
Negative SD square sum	Square sum of negative delay jitters from source to destination
Negative DS square sum	Square sum of negative delay jitters from destination to source

Field	Description
One way results	Uni-direction delay test result, displayed in a UDP jitter or voice test
Max SD delay	Maximum delay from source to destination
Max DS delay	Maximum delay from destination to source
Min SD delay	Minimum delay from source to destination
Min DS delay	Minimum delay from destination to source
Number of SD delay	Number of delays from source to destination
Number of DS delay	Number of delays from destination to source
Sum of SD delay	Sum of delays from source to destination
Sum of DS delay	Sum of delays from destination to source
Square sum of SD delay	Square sum of delays from source to destination
Square sum of DS delay	Square sum of delays from destination to source
SD lost packet(s)	Number of lost packets from the source to the destination
DS lost packet(s)	Number of lost packets from the destination to the source
Lost packet(s) for unknown reason	Number of lost packets for unknown reasons
Voice scores	Voice parameters, displayed only in a voice test
MOS value	MOS value calculated for a voice test
ICPIF value	ICPIF value calculated for a voice test

display nqa statistics

Syntax

display nqa statistics [*admin-name operation-tag*] [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

admin-name operation-tag: Displays statistics of the specified test group. If these two arguments are not specified, statistics of all test groups are displayed. *admin-name* represents the name of the NQA test group administrator who creates the NQA operation, and it is a case-insensitive string of 1 to 32 characters. *operation-tag* represents the test operation tag, and it is a case-insensitive string of 1 to 32 characters.

|: 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 nqa statistics** to display test result statistics for the specified or all test groups.

Statistics cannot be generated until all probe operations in the first test of a test group have finished. If they have not finished and you display statistics by using this command, the statistics are display as all 0s.

If a reaction entry is configured, the command displays the monitoring results of the reaction entry in the period specified by the **statistics interval** command. If the threshold type is average value or the monitored element is ICPIF or MOS for voice tests, the monitoring results are invalid.

Related commands: **statistics interval**.

Examples

Display statistics of UDP jitter tests.

```
<Sysname> display nqa statistics admin test
NQA entry (admin admin, tag test) test statistics:
NO. : 1
Destination IP address: 1.1.1.2
Start time: 2011-01-01 09:33:22.3
Life time: 23 seconds
Send operation times: 100          Receive response times: 100
Min/Max/Average round trip time: 1/11/5
Square-Sum of round trip time: 24360
Extended results:
Packet loss in test: 0%
Failures due to timeout: 0
Failures due to disconnect: 0
Failures due to no connection: 0
Failures due to sequence error: 0
Failures due to internal error: 0
Failures due to other errors: 0
Packet(s) arrived late: 0
UDP-jitter results:
RTT number: 550
Min positive SD: 1          Min positive DS: 1
Max positive SD: 7          Max positive DS: 1
Positive SD number: 220     Positive DS number: 97
Positive SD sum: 283        Positive DS sum: 287
Positive SD average: 1      Positive DS average: 2
Positive SD square sum: 709 Positive DS square sum: 1937
Min negative SD: 2          Min negative DS: 1
Max negative SD: 10         Max negative DS: 1
Negative SD number: 81      Negative DS number: 94
Negative SD sum: 556        Negative DS sum: 191
Negative SD average: 6      Negative DS average: 2
Negative SD square sum: 4292 Negative DS square sum: 967
One way results:
Max SD delay: 5             Max DS delay: 5
```

Min SD delay: 1	Min DS delay: 1
Number of SD delay: 550	Number of DS delay: 550
Sum of SD delay: 1475	Sum of DS delay: 1201
Square sum of SD delay: 5407	Square sum of DS delay: 3959
SD lost packet(s): 0	DS lost packet(s): 0
Lost packet(s) for unknown reason: 0	

Reaction statistics:

Index	Checked Element	Threshold Type	Checked Num	Over-threshold Num
1	jitter-DS	accumulate	90	25
2	jitter-SD	average	-	-
3	OWD-DS	-	100	24
4	OWD-SD	-	100	13
5	packet-loss	accumulate	0	0
6	RTT	accumulate	100	52

Display statistics of voice tests.

<Sysname> display nqa statistics admin test

NQA entry (admin admin, tag test) test statistics:

NO. : 1

Destination IP address: 1.1.1.2

Start time: 2011-01-01 09:33:45.3

Life time: 120 seconds

Send operation times: 10

Receive response times: 10

Min/Max/Average round trip time: 1/12/7

Square-Sum of round trip time: 620

Extended results:

Packet loss in test: 0%

Failures due to timeout: 0

Failures due to disconnect: 0

Failures due to no connection: 0

Failures due to sequence error: 0

Failures due to internal error: 0

Failures due to other errors: 0

Packet(s) arrived late: 0

Voice results:

RTT number: 10

Min positive SD: 3

Min positive DS: 1

Max positive SD: 10

Max positive DS: 1

Positive SD number: 3

Positive DS number: 2

Positive SD sum: 18

Positive DS sum: 2

Positive SD average: 6

Positive DS average: 1

Positive SD square sum: 134

Positive DS square sum: 2

Min negative SD: 3

Min negative DS: 1

Max negative SD: 9

Max negative DS: 1

Negative SD number: 4

Negative DS number: 2

Negative SD sum: 25

Negative DS sum: 2

Negative SD average: 6

Negative DS average: 1

Negative SD square sum: 187

Negative DS square sum: 2

One way results:

```

Max SD delay: 0
Min SD delay: 0
Number of SD delay: 0
Sum of SD delay: 0
Square sum of SD delay: 0
SD lost packet(s): 0
Lost packet(s) for unknown reason: 0

Max DS delay: 0
Min DS delay: 0
Number of DS delay: 0
Sum of DS delay: 0
Square sum of DS delay: 0
DS lost packet(s): 0

Voice scores:
Max MOS value: 4.40
Min MOS value: 4.40
Max ICPIF value: 0
Min ICPIF value: 0

Reaction statistics:
Index   Checked Element   Threshold Type   Checked Num   Over-threshold Num
1       ICPIF             -               -             -
2       MOS               -               -             -

```

Table 35 Command output

Field	Description
No.	Statistics group number
Destination IP address	IP address of the destination
Start time	Time when the test group starts
Life time	Duration of the test, in seconds
Send operation times	Number of probe packets sent
Receive response times	Number of response packets received
Min/Max/Average round trip time	Minimum/maximum/average round-trip time in milliseconds
Square-Sum of round trip time	Square sum of round-trip time
Packet loss in test	Average packet loss ratio
Failures due to timeout	Number of timeout occurrences in a test
Failures due to disconnect	Number of disconnections by the peer
Failures due to no connection	Number of failures to connect with the peer
Failures due to sequence error	Number of failures due to out-of-sequence packets
Failures due to internal error	Number of failures due to internal errors
Failures due to other errors	Failures due to other errors
Packet(s) arrived late	Number of response packets received after a probe times out
UDP-jitter results	UDP jitter test results, available only in UDP jitter tests
Voice results	Voice test results, available only in voice tests
RTT number	Number of response packets received
Min positive SD	Minimum positive delay jitter from source to destination
Min positive DS	Minimum positive delay jitter from destination to source
Max positive SD	Maximum positive delay jitter from source to destination
Max positive DS	Maximum positive delay jitter from destination to source
Positive SD number	Number of positive delay jitters from source to destination

Field	Description
Positive DS number	Number of positive delay jitters from destination to source
Positive SD sum	Sum of positive delay jitters from source to destination
Positive DS sum	Sum of positive delay jitters from destination to source
Positive SD average	Average of positive delay jitters from source to destination
Positive DS average	Average of positive delay jitters from destination to source
Positive SD square sum	Square sum of positive delay jitters from source to destination
Positive DS square sum	Square sum of positive delay jitters from destination to source
Min negative SD	Minimum absolute value among negative delay jitters from source to destination
Min negative DS	Minimum absolute value among negative delay jitters from destination to source
Max negative SD	Maximum absolute value among negative delay jitters from source to destination
Max negative DS	Maximum absolute value among negative delay jitters from destination to source
Negative SD number	Number of negative delay jitters from source to destination
Negative DS number	Number of negative delay jitters from destination to source
Negative SD sum	Sum of absolute values of negative delay jitters from source to destination
Negative DS sum	Sum of absolute values of negative delay jitters from destination to source
Negative SD average	Average absolute value of negative delay jitters from source to destination
Negative DS average	Average absolute value of negative delay jitters from destination to source
Negative SD square sum	Square sum of negative delay jitters from source to destination
Negative DS square sum	Square sum of negative delay jitters from destination to source
One way results	Uni-direction delay test result, displayed on in a UDP Jitter or voice test
Max SD delay	Maximum delay from source to destination
Max DS delay	Maximum delay from destination to source
Min SD delay	Minimum delay from source to destination
Min DS delay	Minimum delay from destination to source
Number of SD delay	Number of delays from source to destination
Number of DS delay	Number of delays from destination to source
Sum of SD delay	Sum of delays from source to destination
Sum of DS delay	Sum of delays from destination to source
Square sum of SD delay	Square sum of delays from source to destination
Square sum of DS delay	Square sum of delays from destination to source

Field	Description
SD lost packet(s)	Number of lost packets from the source to the destination
DS lost packet(s)	Number of lost packets from the destination to the source
Lost packet(s) for unknown reason	Number of lost packets for unknown reasons
Voice scores	Voice parameters, displayed only in a voice test
Max MOS value	Maximum MOS value
Min MOS value	Minimum MOS value
Max ICPIF value	Maximum ICPIF value
Min ICPIF value	Minimum ICPIF value
Reaction statistics	Statistics about the reaction entry in the counting interval
Index	ID of a reaction entry
Checked Element	Monitored element
Threshold Type	Threshold type
Checked Num	Number of targets that have been monitored for data collection
Over-threshold Num	Number of threshold violations

Table 36 Description on the threshold monitoring fields of the display nqa statistics command

Monitored element	Threshold type	Collect data in	Checked Num	Over-threshold Num
probe-duration	accumulate	Probes in the counting interval	Number of finished probes in the counting interval	Number of probes of which the duration exceeds the threshold in the counting interval
	average	N/A	N/A	N/A
	consecutive	Probes in the counting interval	Number of finished probes in the counting interval	Number of probes of which the duration exceeds the threshold in the counting interval
probe-fail	accumulate	Probes in the counting interval	Number of finished probes in the counting interval	Number of probe failures in the counting interval
	consecutive	Probes in the counting interval	Number of finished probes in the counting interval	Number of probe failures in the counting interval
RTT	accumulate	Packets sent in the counting interval	Number of packets sent in the counting interval	Number of packets of which the round-trip time exceeds the threshold in the counting interval
	average	N/A	N/A	N/A

Monitored element	Threshold type	Collect data in	Checked Num	Over-threshold Num
jitter-DS/jitter-SD	accumulate	Packets sent in the counting interval	Number of packets sent in the counting interval	Number of packets of which the one-way delay jitter exceeds the threshold in the counting interval
	average	N/A	N/A	N/A
OWD-DS/OWD-SD	N/A	Packets sent in the counting interval	Number of packets sent in the counting interval	Number of packets of which the one-way delay exceeds the threshold in the counting interval
packet-loss	accumulate	Packets sent in the counting interval	Number of packets sent in the counting interval	Number of packet loss in the counting interval
ICPIF	N/A	N/A	N/A	N/A
MOS	N/A	N/A	N/A	N/A

filename

Syntax

filename *filename*

undo filename

View

FTP operation view

Default level

2: System level

Parameters

filename: Specifies the name of the file transferred between the FTP server and the FTP client. The file name is a case-sensitive string of 1 to 200 characters.

Description

Use **filename** to specify a file to be transferred between the FTP server and the FTP client.

Use **undo filename** to restore the default.

By default, no file is specified.

Examples

Specify the file to be transferred between the FTP server and the FTP client as **config.txt**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] filename config.txt
```

frequency

Syntax

frequency *interval*

undo frequency

View

Any NQA operation view

Default level

2: System level

Parameters

interval: Specifies the interval in milliseconds between two consecutive tests, in the range of 0 to 604800000. The value 0 sets the test group to perform only one test, and not to collect any statistics.

Description

Use **frequency** to configure the interval between two consecutive tests for a test group. When a test group starts, it performs tests one by one at the specified interval. However, if a test is not completed when the interval is reached, no new test starts.

Use **undo frequency** to restore the default.

By default, the interval between two consecutive voice tests is 60000 milliseconds, and the interval between two consecutive tests of other types is 0 milliseconds.

Examples

```
# Configure the ICMP echo test group starts tests one by one at an interval of 1000 milliseconds.
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] frequency 1000
```

history-record enable

Syntax

history-record enable

undo history-record enable

View

Any NQA operation view

Default level

2: System level

Parameters

None

Description

Use **history-record enable** to enable the saving of history records of an NQA test group.

Use **undo history-record enable** to disable the history records saving function.

By default, history records of an NQA test group are not saved.

If the history records saving function is enabled, the system saves the history records. To view the history records of the NQA test group, use the **display nqa history** command.

If the history records saving function is disabled, the system does not save the history records of the NQA test group and the existing history records are also removed.

Related commands: **display nqa history**.

Examples

Enable the history records saving function of an NQA test group.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] history-record enable
```

history-record keep-time

Syntax

history-record keep-time *keep-time*

undo history-record keep-time

View

Any NQA operation view

Default level

2: System level

Parameters

keep-time: Specifies how long the history records can be saved. The time is in the range of 1 to 1440 minutes.

Description

Use **history-record keep-time** to set the lifetime of the history records in an NQA test group.

Use **undo history-record keep-time** to restore the default.

By default, the history records in an NQA test group are kept for 120 minutes.

When an NQA test completes, the timing starts. All records are removed when the lifetime is reached.

Examples

Configure the lifetime of the history records in an NQA test group as 100 minutes.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] history-record keep-time 100
```

history-record number

Syntax

history-record number *number*

undo history-record number

View

Any NQA operation view

Default level

2: System level

Parameters

number: Specifies the maximum number of history records that can be saved in a test group. The value is in the range of 0 to 50.

Description

Use **history-record number** to configure the maximum number of history records that can be saved in a test group.

Use **undo history-record number** to restore the default.

By default, the maximum number of records that can be saved in a test group is 50.

If the number of history records in a test group exceeds the maximum number, the earliest history record is removed.

Examples

```
# Configure the maximum number of history records that can be saved in a test group as 10.
```

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

```
[Sysname] nqa entry admin test
```

```
[Sysname-nqa-admin-test] type icmp-echo
```

```
[Sysname-nqa-admin-test-icmp-echo] history-record number 10
```

http-version

Syntax

http-version v1.0

undo http-version

View

HTTP operation view

Default level

2: System level

Parameters

v1.0: Uses HTTP version 1.0 in an HTTP test.

Description

Use **http-version** to configure the HTTP version used in an HTTP test.

Use **undo http-version** to restore the default.

By default, HTTP 1.0 is used in an HTTP test.

Examples

```
# Configure the HTTP version as 1.0 in an HTTP test.
```

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

```
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type http
[Sysname-nqa-admin-test-http] http-version v1.0
```

mode

Syntax

mode { active | passive }

undo mode

View

FTP operation view

Default level

2: System level

Parameters

active: Sets the data transmission mode to active for FTP tests. In this mode, the FTP server initiates a data connection request.

passive: Sets the data transmission mode to passive for FTP tests. In this mode, a client initiates a data connection request.

Description

Use **mode** to set the data transmission mode for FTP tests.

Use **undo mode** to restore the default.

By default, the data transmission mode is **active**.

Examples

Set the data transmission mode to passive for FTP tests.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] mode passive
```

next-hop

Syntax

next-hop *ip-address*

undo next-hop

View

ICMP echo operation view

Default level

2: System level

Parameters

ip-address: Specifies the IP address of the next hop.

Description

Use **next-hop** to configure the next hop IP address for ICMP echo requests of a test group.

Use **undo next-hop** to remove the configured next hop IP address.

By default, no next hop IP address is configured.

Examples

Configure the next hop IP address as 10.1.1.1.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] next-hop 10.1.1.1
```

nqa

Syntax

nqa entry *admin-name operation-tag*

undo nqa { **all** | **entry** *admin-name operation-tag* }

View

System view

Default level

2: System level

Parameters

admin-name: Specifies the name of the NQA test group administrator who creates the NQA test operation, a case-insensitive string of 1 to 32 characters, with "-" excluded.

operation-tag: Specifies the tag of a test operation, a case-insensitive string of 1 to 32 characters, with "-" excluded.

all: Removes all NQA test groups.

Description

Use **nqa** to create an NQA test group and enter NQA test group view.

Use **undo nqa** to remove the test group.

If the operation has been configured for the test group, you directly enter NQA operation view when you execute the **nqa** command.

Examples

Create an NQA test group whose administrator name is **admin** and whose operation tag is **test** and enter NQA test group view.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test]
```

nqa agent enable

Syntax

```
nqa agent enable  
undo nqa agent enable
```

View

System view

Default level

2: System level

Parameters

None

Description

Use **nqa agent enable** to enable the NQA client.

Use **undo nqa agent enable** to disable the NQA client and stop all tests being performed.

By default, the NQA client is enabled.

Related commands: **nqa server enable**.

Examples

```
# Enable the NQA client.  
<Sysname> system-view  
[Sysname] nqa agent enable
```

nqa agent max-concurrent

Syntax

```
nqa agent max-concurrent number  
undo nqa agent max-concurrent
```

View

System view

Default level

2: System level

Parameters

number: Specifies the maximum number of tests that the NQA client can simultaneously perform. The value is in the range of 1 to 5.

Description

Use **nqa agent max-concurrent** to configure the maximum number of tests that the NQA client can simultaneously perform.

Use **undo nqa agent max-concurrent** to restore the default.

By default, the maximum number is 2.

From the beginning to the end of a test, the NQA test is in test status. From the end of a test to the beginning of the next test, the NQA test is in waiting status.

Examples

Configure the maximum number of tests that the NQA client can simultaneously perform as 5.

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

```
[Sysname] nqa agent max-concurrent 5
```

nqa schedule

Syntax

```
nqa schedule admin-name operation-tag start-time { hh:mm:ss [ yyyy/mm/dd ] | now } lifetime  
{ lifetime | forever }
```

```
undo nqa schedule admin-name operation-tag
```

View

System view

Default level

2: System level

Parameters

admin-name: Specifies the name of the NQA test group administrator who creates the NQA test operation. The name is a case-insensitive string of 1 to 32 characters.

operation-tag: Specifies the test operation tag, a case-insensitive string of 1 to 32 characters.

start-time: Specifies the start time and date of a test group.

hh:mm:ss: Specifies the start time of a test group.

yyyy/mm/dd: Specifies the start date of a test group. The default value is the current system time, and *yyyy* is in the range of 2000 to 2035.

now: Starts the tests for a test group immediately.

lifetime: Specifies the duration of the test operation.

lifetime: Specifies the duration of the test operation in seconds, in the range of 1 to 2147483647.

forever: Specifies that the tests are performed for a test group forever.

Description

Use **nqa schedule** to configure the test start time and test duration for a test group.

Use **undo nqa schedule** to stop the test for the test group.

You cannot enter test group view or operation view after a test group is scheduled.

A test group performs a test when the system time is between the start time and the end time (the start time plus test duration). If the system time is behind the start time when you execute the **nqa schedule** command, a test is started when the system time reaches the start time. If the system time is between the start time and the end time, a test is started immediately. If the system time is ahead of the end time, no test is started. To view the current system time, use the **display clock** command.

Related commands: **display clock** (*Fundamentals Command Reference*).

Examples

Start the tests for the test group with the administrator name **admin** and operation tag **test**. The start time and duration of the test group are 08:08:08 2011/01/08 and 1000 seconds.

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

```
[Sysname] nqa schedule admin test start-time 08:08:08 2011/01/08 lifetime 1000
```

operation (FTP operation view)

Syntax

operation { get | put }

undo operation

View

FTP operation view

Default level

2: System level

Parameters

get: Obtains a file from the FTP server.

put: Transfers a file to the FTP server.

Description

Use **operation** to configure the FTP operation type.

Use **undo operation** to restore the default.

By default, the FTP operation type is **get**.

Examples

Configure the FTP operation type as **put**.

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

```
[Sysname] nqa entry admin test
```

```
[Sysname-nqa-admin-test] type ftp
```

```
[Sysname-nqa-admin-test-ftp] operation put
```

operation (HTTP operation view)

Syntax

operation { get | post }

undo operation

View

HTTP operation view

Default level

2: System level

Parameters

get: Obtains data from the HTTP server.

post: Transfers data to the HTTP server.

Description

Use **operation** to configure the HTTP operation type.

Use **undo operation** to restore the default.

By default, the HTTP operation type is **get**.

Examples

```
# Configure the HTTP operation type as post.
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type http
[Sysname-nqa-admin-test-http] operation post
```

operation interface

Syntax

operation interface *interface-type interface-number*

undo operation interface

View

DHCP operation view

Default level

2: System level

Parameters

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

Description

Use **operation interface** to specify the interface to perform a DHCP test. The specified interface must be up. Otherwise, no probe packets can be sent out.

Use **undo operation interface** to restore the default.

By default, no interface is specified to perform a DHCP test.

Examples

```
# Specify the interface to perform a DHCP test as VLAN-interface 2.
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type dhcp
[Sysname-nqa-admin-test-dhcp] operation interface vlan-interface 2
```

password (FTP operation view)

Syntax

password [**cipher** | **simple**] *password*

undo password

View

FTP operation view

Default level

2: System level

Parameters

cipher: Sets a ciphertext password.

simple: Sets a plaintext password.

password: Specifies a password used to log in to the FTP server. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 32 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 73 characters. If neither **cipher** nor **simple** is specified, you set a plaintext password string.

Description

Use **password** to configure a password used to log onto the FTP server.

Use **undo password** to remove the configured password.

By default, no password is configured for logging onto the FTP server.

The password set in either plaintext or ciphertext is saved in ciphertext in the configuration file.

Related commands: **username** and **operation**.

Examples

Configure the password used for logging in to the FTP server as **ftpuser**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] password ftpuser
```

probe count

Syntax

probe count *times*

undo probe count

View

DHCP, DNS, DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter operation view

Default level

2: System level

Parameters

times: Specifies the number of probe operations per test, in the range of 1 to 15.

Description

Use **probe count** to configure the number of probe operations to be performed per test.

Use **undo probe count** to restore the default.

By default, one probe operation is performed in an NQA test.

In different test types, probe operation has the following different meanings:

- During a TCP or DLSw test, one probe operation means setting up one connection.
- During a UDP jitter or a voice test, one probe operation means continuously sending a specific number of probe packets. The number of probe packets is configurable with the **probe packet-number** command.
- During an FTP, HTTP, DHCP, or DNS test, one probe operation means uploading or downloading a file, obtaining a web page, obtaining an IP address through DHCP, or translating a domain name to an IP address.
- During an ICMP echo or UDP echo test, one probe operation means sending an ICMP echo request or a UDP packet.
- During an SNMP test, one probe operation means sending one SNMPv1 packet, one SNMPv2C packet, and one SNMPv3 packet.

If more than one probe operation is to be performed in a test, the system starts a second probe operation when it receives responses to packets sent in the first probe operation, or when the probe timeout time expires.

This command is not supported by voice tests. Only one probe operation is performed per voice test.

Examples

Configure the ICMP test group to perform 10 probe operations per test.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] probe count 10
```

probe packet-interval

Syntax

```
probe packet-interval packet-interval
undo probe packet-interval
```

View

UDP jitter, voice operation view

Default level

2: System level

Parameters

packet-interval: Specifies the interval for sending packets per probe operation, in the range of 10 to 60000 milliseconds.

Description

Use **probe packet-interval** to configure the interval for sending packets per probe operation.

Use **undo probe-interval** to restore the default.

By default, the interval is 20 milliseconds.

Examples

Configure the UDP jitter test group to send packets at an interval of 100 milliseconds during each probe operation.

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

```
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] probe packet-interval 100
```

probe packet-number

Syntax

probe packet-number *packet-number*

undo probe packet-number

View

UDP jitter, voice operation view

Default level

2: System level

Parameters

packet-number: Specifies the number of packets to be sent per probe operation. The value is in the range of 10 to 1000 for each probe operation in one UDP jitter test, and 10 to 60000 for each probe operation in one voice test.

Description

Use **probe packet-number** to configure the number of packets to be sent per probe during one UDP jitter or voice test.

Use **undo probe packet-number** to restore the default.

By default, the number of packets to be sent per probe is 10 in one UDP jitter test and 1000 in one voice test.

Examples

Configure the UDP jitter test group to send 100 packets per probe.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] probe packet-number 100
```

probe packet-timeout

Syntax

probe packet-timeout *packet-timeout*

undo probe packet-timeout

View

UDP jitter, voice operation view

Default level

2: System level

Parameters

packet-timeout: Specifies the timeout time in milliseconds for waiting for responses in a UDP jitter or voice test. The value is in the range of 10 to 3600000.

Description

Use **probe packet-timeout** to configure the timeout time for waiting for a response in a UDP jitter or voice test.

Use **undo probe packet-timeout** to restore the default.

By default, the timeout time in a UDP jitter test is 3000 milliseconds, the timeout time in a voice test is 5000 milliseconds.

Examples

Configure the timeout time for waiting for a response in a UDP jitter test as 100 milliseconds.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] probe packet-timeout 100
```

probe timeout

Syntax

probe timeout *timeout*

undo probe timeout

View

DHCP, DNS, DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo operation view

Default level

2: System level

Parameters

timeout: Specifies the timeout time in milliseconds for a probe operation. The value is in the range of 10 to 86400000 for an FTP or HTTP probe operation, and 10 to 3600000 for a DHCP, DNS, DLSw, ICMP echo, SNMP, TCP, or UDP echo probe operation.

Description

Use **probe timeout** to configure the timeout time for a probe operation. When a probe operation does not complete within the period, the probe operation is timed out.

Use **undo probe timeout** to restore the default.

By default, the timeout time is 3000 milliseconds for a probe operation.

This command is not supported by UDP jitter or voice tests.

Examples

Configure the timeout time for a DHCP probe operation as 10000 milliseconds.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type dhcp
[Sysname-nqa-admin-test-dhcp] probe timeout 10000
```

reaction checked-element icpif

Syntax

```
reaction item-number checked-element icpif threshold-value upper-threshold lower-threshold  
[ action-type { none | trap-only } ]
```

```
undo reaction item-number
```

View

Voice operation view

Default level

2: System level

Parameters

item-number: Specifies a reaction entry ID, in the range of 1 to 10.

threshold-value: Specifies threshold values.

upper-threshold: Specifies an upper threshold, in the range of 1 to 100.

lower-threshold: Specifies a lower threshold, in the range of 1 to 100. It must not be greater than the upper threshold.

action-type: Specifies what action to be triggered to react to certain measurement conditions and it defaults to **none**.

none: Specifies to only record events for terminal display, and not to send any trap messages.

trap-only: Specifies to record events and send SNMP trap messages.

Description

Use **reaction checked-element icpif** to configure a reaction entry for monitoring the ICPIF value in a voice test of an NQA operation. You cannot edit a reaction entry. To change the attributes in a reaction entry, use **undo reaction** to delete this entire entry and start over.

Use **undo reaction** to delete the specified reaction entry.

By default, no reaction entry for monitoring ICPIF values is configured.

Examples

Create reaction entry 1 for monitoring the ICPIF value in each voice test. Set the upper threshold to 50 and lower threshold to 5. Before the NQA test group starts, the initial state of the reaction entry is invalid. After each test, the ICPIF value is checked. If it is out of the threshold range, the state of the reaction entry is set to over-threshold. Otherwise, the state is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the network management server.

```
<Sysname> system-view  
[Sysname] nqa entry admin test  
[Sysname-nqa-admin-test] type voice  
[Sysname-nqa-admin-test-voice] reaction 1 checked-element icpif threshold-value 50 5  
action-type trap-only
```

reaction checked-element { jitter-ds | jitter-sd }

Syntax

```
reaction item-number checked-element { jitter-ds | jitter-sd } threshold-type { accumulate  
accumulate-occurrences | average } threshold-value upper-threshold lower-threshold [ action-type  
{ none | trap-only } ]
```

```
undo reaction item-number
```

View

UDP jitter, voice operation view

Default level

2: System level

Parameters

item-number: Specifies a reaction entry ID, in the range of 1 to 10.

jitter-ds: Specifies destination-to-source delay jitter of each probe packet as the monitored element.

jitter-sd: Specifies source-to-destination delay jitter of each probe packet as the monitored element.

threshold-type: Specifies a threshold type.

accumulate *accumulate-occurrences*: Specifies the total number of threshold violations in a test. The value is in the range of 1 to 14999 for UDP jitter tests, and 1 to 59999 for voice tests.

average: Specifies to check the average one-way delay jitter in each test.

threshold-value: Specifies threshold values in milliseconds.

upper-threshold: Specifies an upper threshold, in the range of 0 to 3600000.

lower-threshold: Specifies a lower threshold, in the range of 0 to 3600000. It must not be greater than the upper threshold.

action-type: Specifies what action to be triggered to react to certain measurement conditions and it defaults to **none**.

none: Specifies to only record events for terminal display, and not to send any trap messages.

trap-only: Specifies to record events and send SNMP trap messages.

Description

Use **reaction checked-element { jitter-ds | jitter-sd }** to configure a reaction entry for monitoring one-way delay jitter in each test of an NQA operation. You cannot edit a reaction entry. To change the attributes in a reaction entry, use **undo reaction** to delete this entire entry and start over.

Use **undo reaction** to delete the specified reaction entry.

By default, no reaction entry for monitoring one-way delay jitter is configured.

Only successful probe packets are monitored. The data of a failed probe packet is not counted.

Examples

```
# Create reaction entry 1 for monitoring the average destination-to-source delay jitter of UDP jitter probe  
packets. Set the upper threshold to 50 milliseconds, and the lower threshold to 5 milliseconds. Before the  
NQA test group starts, the initial state of the reaction entry is invalid. After each test, the average  
destination-to-source delay jitter is checked. If it is out of the threshold range, the state of the reaction
```

entry is set to over-threshold. Otherwise, the state is set to below-threshold. Once state of the reaction entry changes, a trap message is generated and sent to the network management server.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] reaction 1 checked-element jitter-ds threshold-type
average threshold-value 50 5 action-type trap-only
```

Create reaction entry 2 for monitoring the destination-to-source delay jitter of UDP jitter probe packets. Set the upper threshold to 50 milliseconds, and the lower threshold to 5 milliseconds. Before the NQA test group starts, the initial state of the reaction entry is invalid. After each test, the destination-to-source delay jitter is checked against the threshold range. If the total number of threshold violations exceeds 100 (included), the state of the entry is set to over-threshold. Otherwise, the state of the entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the network management server.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] reaction 2 checked-element jitter-ds threshold-type
accumulate 100 threshold-value 50 5 action-type trap-only
```

reaction checked-element mos

Syntax

```
reaction item-number checked-element mos threshold-value upper-threshold lower-threshold
[ action-type { none | trap-only } ]
```

```
undo reaction item-number
```

View

Voice operation view

Default level

2: System level

Parameters

item-number: Specifies a reaction entry ID, in the range of 1 to 10.

threshold-value: Specifies threshold values.

upper-threshold: Specifies an upper threshold, in the range of 1 to 500.

lower-threshold: Specifies a lower threshold, in the range of 1 to 500. It must not be greater than the upper threshold.

action-type: Specifies what action to be triggered to react to certain measurement conditions and it defaults to **none**.

none: Specifies to only record events for terminal display, and not to send any trap messages.

trap-only: Specifies to record events and send SNMP trap messages.

Description

Use **reaction checked-element mos** to configure a reaction entry for monitoring the MOS value in each voice test of an NQA operation. You cannot edit a reaction entry. To change the attributes in a reaction entry, use **undo reaction** to delete this entire entry and start over.

Use **undo reaction** to delete the specified reaction entry.

By default, no reaction entry for monitoring the MOS value is configured.

For the MOS threshold, the number is expressed in three digits representing ones, tenths, and hundredths. For example, to express a MOS threshold of 1, enter 100.

Examples

Create reaction entry 1 for monitoring the MOS value of each voice test. Set the upper threshold to 2, and lower threshold to 1. Before the NQA test group starts, the initial state of the reaction entry is invalid. After each test, the MOS value is checked. If it is out of the threshold range, the state of the reaction entry is set to over-threshold. Otherwise, the state is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the network management server.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type voice
[Sysname-nqa-admin-test-voice] reaction 1 checked-element mos threshold-value 200 100
action-type trap-only
```

reaction checked-element { owd-ds | owd-sd }

Syntax

reaction *item-number* **checked-element** { **owd-ds** | **owd-sd** } **threshold-value** *upper-threshold*
lower-threshold

undo reaction *item-number*

View

UDP jitter, voice operation view

Default level

2: System level

Parameters

item-number: Specifies a reaction entry ID, in the range of 1 to 10.

owd-ds: Specifies the destination-to-source delay of each probe packet as the monitored element.

owd-sd: Specifies the source-to-destination delay of each probe packet as the monitored element.

threshold-value: Specifies threshold values in milliseconds.

upper-threshold: Specifies an upper threshold, in the range of 0 to 3600000.

lower-threshold: Specifies a lower threshold, in the range of 0 to 3600000. It must not be greater than the upper threshold.

Description

Use **reaction checked-element { owd-ds | owd-sd }** to configure a reaction entry for monitoring the one-way delay. You cannot edit a reaction entry. To change the attributes in a reaction entry, use **undo reaction** to delete this entire entry and start over.

Use **undo reaction** to delete the specified reaction entry.

By default, no reaction entry for monitoring the one-way delay is configured.

Only successful probe packets are monitored. The data of a failed probe packet is not counted.

No actions can be configured for a reaction entry of monitoring one-way delays. The monitoring results and statistics, however, can be displayed by the **display nqa reaction counters** and **display nqa statistics** commands.

Examples

Create reaction entry 1 for monitoring the destination-to-source delay of every UDP jitter probe packet. Set the upper threshold to 50 milliseconds and lower threshold to 5 milliseconds. Before the NQA test group starts, the initial state of the reaction entry is invalid. The destination-to-source delay is calculated after the response to the probe packet arrives. If the delay is out of the threshold range, the state of the reaction entry is set to over-threshold. Otherwise, the state is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the network management server.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] reaction 1 checked-element owd-ds threshold-value 50
5
```

reaction checked-element packet-loss

Syntax

reaction *item-number* **checked-element packet-loss threshold-type accumulate** *accumulate-occurrences*
[**action-type** { **none** | **trap-only** }]

undo reaction *item-number*

View

UDP jitter, voice operation view

Default level

2: System level

Parameters

item-number: Specifies a reaction entry ID, in the range of 1 to 10.

threshold-type: Specifies a threshold type.

accumulate *accumulate-occurrences*: Specifies the total number of lost packets in a test. The value is in the range of 1 to 15000 for UDP jitter tests and 1 to 60000 for voice tests.

action-type: Specifies what action to be triggered to react to certain measurement conditions and it defaults to **none**.

none: Specifies to only record events for terminal display, and not to send any trap messages.

trap-only: Specifies to record events and send SNMP trap messages.

Description

Use **reaction checked-element packet-loss** to configure a reaction entry for monitoring the packet loss in each test of an NQA operation. You cannot edit a reaction entry. To change the attributes in a reaction entry, use **undo reaction** to delete this entire entry and start over.

Use **undo reaction** to delete the specified reaction entry.

By default, no reaction entry for monitoring the packet loss is configured.

Examples

Create reaction entry 1 for monitoring the packet loss in each UDP jitter test. Before the NQA test group starts, the initial state of the reaction entry is invalid. After each test, the packet loss is checked. If the total number of lost packets exceeds 100 (included), the state of the reaction entry is set to over-threshold. Otherwise, the state is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the network management server.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] reaction 1 checked-element packet-loss
threshold-type accumulate 100 action-type trap-only
```

reaction checked-element probe-duration

Syntax

```
reaction item-number checked-element probe-duration threshold-type { accumulate
accumulate-occurrences | average | consecutive consecutive-occurrences } threshold-value
upper-threshold lower-threshold [ action-type { none | trap-only } ]
undo reaction item-number
```

View

DHCP, DLSw, DNS, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo operation view

Default level

2: System level

Parameters

item-number: Specifies a reaction entry ID, in the range of 1 to 10.

threshold-type: Specifies a threshold type.

accumulate *accumulate-occurrences*: Specifies the total number of threshold violations in a test. The value is in the range of 1 to 15.

average: Specifies to check the average probe duration in each test.

consecutive *consecutive-occurrences*: Specifies the number of consecutive threshold violations since the NQA test group starts. The value is in the range of 1 to 16.

threshold-value: Specifies threshold values in milliseconds.

upper-threshold: Specifies an upper threshold, in the range of 0 to 3600000.

lower-threshold: Specifies a lower threshold, in the range of 0 to 3600000. It must not be greater than the upper threshold.

action-type: Specifies what action to be triggered to react to certain measurement conditions and it defaults to **none**.

none: Specifies to only record events for terminal display, and not to send any trap messages.

trap-only: Specifies to record events and send SNMP trap messages. This keyword is not supported in DNS test view.

Description

Use **reaction checked-element probe-duration** to configure a reaction entry for monitoring the probe duration. You cannot edit a reaction entry. To change the attributes in a reaction entry, use **undo reaction** to delete this entire entry and start over.

Use **undo reaction** to delete the specified reaction entry.

By default, no reaction entry for monitoring the probe duration is configured.

Only successful probes are monitored. The duration of a failed probe is not counted.

Examples

Create reaction entry 1 for monitoring the average duration of ICMP echo probes in a test. Set the upper threshold to 50 milliseconds and lower threshold to 5 milliseconds. Before the NQA test group starts, the initial state of the reaction entry is invalid. After each test, the average probe duration is checked. If it is out of the threshold range, the state is set to over-threshold. Otherwise, the state of the reaction entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the network management server.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-duration
threshold-type average threshold-value 50 5 action-type trap-only
```

Create reaction entry 2 for monitoring the duration of ICMP echo probes in a test. Set the upper threshold to 50 milliseconds, and the lower threshold to 5 milliseconds. Before the NQA test group starts, the initial state of the reaction entry is invalid. After each test, the probe duration is checked against the threshold range. If the total number of threshold violations exceeds 10 (included), the state of the entry is set to over-threshold. Otherwise, the state of the entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the network management server.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] reaction 2 checked-element probe-duration
threshold-type accumulate 10 threshold-value 50 5 action-type trap-only
```

Create reaction entry 3 for monitoring the duration time of ICMP echo probes. Set the upper threshold to 50 milliseconds, and the lower threshold to 5 milliseconds. Before the NQA test group starts, the initial state of the reaction entry is invalid. The probe duration is checked against the threshold range for each probe. If a threshold violation occurs consecutively for 10 times or more since the test group starts, the state of the entry is set to over-threshold. Otherwise, the state of the entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the network management server.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] reaction 3 checked-element probe-duration
threshold-type consecutive 10 threshold-value 50 5 action-type trap-only
```

reaction checked-element probe-fail (for trap)

Syntax

```
reaction item-number checked-element probe-fail threshold-type { accumulate accumulate-occurrences  
| consecutive consecutive-occurrences } [ action-type { none | trap-only } ]  
undo reaction item-number
```

View

DHCP, DLSw, DNS, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo operation view

Default level

2: System level

Parameters

item-number: Specifies a reaction entry ID, in the range of 1 to 10.

threshold-type: Specifies a threshold type.

accumulate *accumulate-occurrences*: Specifies the total number of probe failures in a test. The value is in the range of 1 to 15.

consecutive *consecutive-occurrences*: Specifies the number of consecutive probe failures since the NQA test group starts. The value is in the range of 1 to 16.

action-type: Specifies what action to be triggered to react to certain measurement conditions and it defaults to **none**.

none: Specifies to only record events for terminal display, and not to send any trap messages.

trap-only: Specifies to record events and send SNMP trap messages. This keyword is not supported in DNS test view.

Description

Use **reaction checked-element probe-fail** to configure a reaction entry for monitoring the probe failures. You cannot edit a reaction entry. To change the attributes in a reaction entry, use **undo reaction** to delete this entire entry and start over.

Use **undo reaction** to delete the specified reaction entry.

By default, no reaction entry for monitoring probe failures is configured.

Examples

Create reaction entry 1 for monitoring the probe failures in ICMP echo tests. Before the NQA test group starts, the initial state of the reaction entry is invalid. After each test, if the total number of probe failures exceeds 10 (included), the state of the entry is set to over-threshold. Otherwise, the state of the entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the network management server.

```
<Sysname> system-view  
[Sysname] nqa entry admin test  
[Sysname-nqa-admin-test] type icmp-echo  
[Sysname-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type  
accumulate 10 action-type trap-only
```

Create reaction entry 2 for monitoring the probe failures in ICMP echo tests. Before the NQA test group starts, the initial state of the reaction entry is invalid. If probe failure occurs consecutively for 10 times or more since the test group starts, the state of the entry is set to over-threshold. Otherwise, the state of the

entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the network management server.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] reaction 2 checked-element probe-fail threshold-type
consecutive 10 action-type trap-only
```

reaction checked-element probe-fail (for trigger)

Syntax

reaction *item-number* **checked-element probe-fail threshold-type consecutive** *consecutive-occurrences*
action-type trigger-only

undo reaction *item-number*

View

DHCP, DNS, DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo operation view

Default level

2: System level

Parameters

item-number: Specifies a reaction entry ID, in the range of 1 to 10.

threshold-type: Specifies a threshold type.

consecutive *consecutive-occurrences*: Specifies the number of consecutive probe failures since the test group starts. The value is in the range of 1 to 16.

action-type: Specifies what actions to be triggered to react to certain measurement conditions.

trigger-only: Triggers other modules to react to certain conditions.

Description

Use **reaction checked-element probe-fail** to configure a reaction entry for monitoring the probe results of the current test group. If the number of consecutive probe failures reaches the threshold, collaboration with other modules is triggered. You cannot edit a reaction entry. To change the attributes in a reaction entry, use **undo reaction** to delete this entire entry and start over.

Use **undo reaction** to remove the specified reaction entry.

By default, no reaction entries are configured.

The collaboration function is not supported by UDP jitter or voice tests.

Related commands: **track** (High Availability Command Reference).

Examples

Create reaction entry 1. If probe failure occurs consecutively for 3 times, collaboration with other modules is triggered.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type tcp
[Sysname-nqa-admin-test-tcp] reaction 1 checked-element probe-fail threshold-type
consecutive 3 action-type trigger-only
```

reaction checked-element rtt

Syntax

```
reaction item-number checked-element rtt threshold-type { accumulate accumulate-occurrences | average } threshold-value upper-threshold lower-threshold [ action-type { none | trap-only } ]  
undo reaction item-number
```

View

UDP jitter, voice operation view

Default level

2: System level

Parameters

item-number: Specifies a reaction entry ID, in the range of 1 to 10.

threshold-type: Specifies a threshold type.

accumulate *accumulate-occurrences*: Specifies the total number of threshold violations in a test. The value is in the range of 1 to 15000 for UDP jitter tests and 1 to 60000 for voice tests.

average: Specifies to check the packet average round-trip time in a test.

threshold-value: Specifies threshold values in milliseconds.

upper-threshold: Specifies an upper threshold, in the range of 0 to 3600000.

lower-threshold: Specifies a lower threshold, in the range of 0 to 3600000. It must not be greater than the upper threshold.

action-type: Specifies what action to be triggered to react to certain measurement conditions and it defaults to **none**.

none: Specifies to only record events for terminal display, and not to send any trap messages.

trap-only: Specifies to record events and send SNMP trap messages.

Description

Use **reaction checked-element rtt** to configure a reaction entry for monitoring packet round-trip time. You cannot edit a reaction entry. To change the attributes in a reaction entry, use **undo reaction** to delete this entire entry and start over.

Use **undo reaction** to delete the specified reaction entry.

By default, no reaction entry for monitoring packet round-trip time is configured.

Only successful probe packets are monitored. The data of a failed probe packet is not counted.

Examples

Create reaction entry 1 for monitoring the average round-trip time of UDP jitter probe packets. Set the upper threshold to 50 milliseconds and lower threshold to 5 milliseconds. Before the NQA test group starts, the initial state of the reaction entry is invalid. After each test, the average packet round-trip time is checked. If it is out of the threshold range, the state is set to over-threshold. Otherwise, the state is set to below-threshold. Once the reaction entry state changes, a trap message is generated and sent to the network management server.

```
<Sysname> system-view  
[Sysname] nqa entry admin test  
[Sysname-nqa-admin-test] type udp-jitter
```

```
[Sysname-nqa-admin-test-udp-jitter] reaction 1 checked-element rtt threshold-type
average threshold-value 50 5 action-type trap-only
```

Create reaction entry 2 for monitoring the round-trip time of UDP jitter probe packets. Set the upper threshold to 50 milliseconds, and lower threshold to 5 milliseconds. Before the NQA test group starts, the initial state of the reaction entry is invalid. After each test, the packet round-trip time is checked against the threshold range. If the total number of threshold violations exceeds 100 (included), the state of the entry is set to over-threshold. Otherwise, the state of the entry is set to below-threshold. Once the state of the reaction entry changes, a trap message is generated and sent to the network management server.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] reaction 1 checked-element rtt threshold-type
accumulate 100 threshold-value 50 5 action-type trap-only
```

reaction trap

Syntax

```
reaction trap { probe-failure consecutive-probe-failures | test-complete | test-failure
cumulate-probe-failures }
```

```
undo reaction trap { probe-failure | test-complete | test-failure }
```

View

Any NQA operation view

Default level

2: System level

Parameters

probe-failure *consecutive-probe-failures*: Sends a trap to the network management server if the number of consecutive probe failures in one test is greater than or equal to *consecutive-probe-failures*. The value for *consecutive-probe-failures* is in the range of 1 to 15. During the test, the system counts the number of consecutive probe failures after each probe operation, so multiple traps might be sent.

test-complete: Sends a trap to indicate that the test is completed.

test-failure *cumulate-probe-failures*: Sends a trap if the total probe failures in an test is greater than or equal to *cumulate-probe-failures*. The value for *cumulate-probe-failures* is in the range of 1 to 15. The system counts the total probe failures after the test completes, so one trap at most is sent.

Description

Use **reaction trap** to configure the sending of traps to the network management server under specified conditions.

Use **undo reaction trap** to restore the default.

By default, no traps are sent to the network management server.

Only the **reaction trap test-complete** command is supported by voice tests.

Examples

Configure the system to send a trap if consecutive probe failures in an ICMP echo test is greater than or equal to 5.

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

```
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] reaction trap probe-failure 5
```

resolve-target

Syntax

resolve-target *domain-name*

undo resolve-target

View

DNS operation view

Default level

2: System level

Parameters

domain-name: Specifies the domain name to be resolved. It is a case-insensitive string separated by dots (.), each part consisting of 1 to 63 characters. The total length must be within 255 characters. Valid characters in a part include letters, digits, hyphens (-), and underscores (_).

Description

Use **resolve-target** to set the domain name for a DNS test.

Use **undo resolve-target** to restore the default.

By default, no domain name is configured.

Examples

```
# Set the domain name for DNS resolution to domain1.
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type dns
[Sysname-nqa-admin-test-dns] resolve-target domain1
```

route-option bypass-route

Syntax

route-option bypass-route

undo route-option bypass-route

View

DLSw, DNS, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice operation view

Default level

2: System level

Parameters

None

Description

Use **route-option bypass-route** to enable the routing table bypass function to test the direct connectivity to the direct destination.

Use **undo route-option bypass-route** to disable the routing table bypass function.

By default, the routing table bypass function is disabled.

When the routing table bypass function is enabled, the routing table is not searched, and the packet is sent directly to the destination in a directly connected network.

Examples

Enable the routing table bypass function.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] route-option bypass-route
```

source interface

Syntax

source interface *interface-type interface-number*

undo source interface

View

ICMP echo operation view

Default level

2: System level

Parameters

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

Description

Use **source interface** to configure the source interface for ICMP echo request packets. The ICMP echo request packets take the IP address of the source interface as their source IP address. The specified source interface must be up. Otherwise, no ICMP echo requests can be sent out.

Use **undo source interface** to restore the default.

By default, no source interface is configured for ICMP echo request packets.

If you configure both the **source interface** command and the **source ip** command, the **source ip** command takes effect.

Related commands: **source ip**.

Examples

Specify the IP address of interface VLAN-interface 2 as the source IP address of ICMP echo request packets.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] source interface vlan-interface 2
```

source ip

Syntax

source ip *ip-address*

undo source ip

View

DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice operation view

Default level

2: System level

Parameters

ip-address: Specifies the source IP address of a test operation.

Description

Use **source ip** to configure the source IP address of probe packets. The specified source IP address must be the IP address of a local interface. The local interface must be up. Otherwise, no probe packets can be sent out.

Use **undo source ip** to remove the configured source address. The IP address of the interface that sends a probe packet serves as the source IP address of the probe packet.

By default, no source IP address is configured for probe packets.

If you configure both the **source interface** command and the **source ip** command, the **source ip** command takes effect.

Related commands: **source interface**.

Examples

Configure the source IP address of the ICMP echo packets as 10.1.1.1.

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

```
[Sysname] nqa entry admin test
```

```
[Sysname-nqa-admin-test] type icmp-echo
```

```
[Sysname-nqa-admin-test-icmp-echo] source ip 10.1.1.1
```

source port

Syntax

source port *port-number*

undo source port

View

SNMP, UDP echo, UDP jitter, voice operation view

Default level

2: System level

Parameters

port-number: Specifies the source port number of probe packets, in the range of 1 to 50000.

Description

Use **source port** to configure the source port of probe packets.

Use **undo source port** to remove the configured port number.

By default, no source port number is configured.

Examples

Configure port 8000 as the source port of probe packets in the UDP echo test group.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-echo
[Sysname-nqa-admin-test-udp-echo] source port 8000
```

statistics hold-time

Syntax

statistics hold-time *hold-time*

undo statistics hold-time

View

DLSw, DNS, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice operation view

Default level

2: System level

Parameters

hold-time: Specifies the hold time of a statistics group in minutes, in the range of 1 to 1440.

Description

Use **statistics hold-time** to configure the hold time of statistics groups for a test group. A statistics group is deleted when its hold time expires.

Use **undo statistics hold-time** to restore the default.

By default, the hold time of a statistics group is 120 minutes.

This command is not supported by DHCP tests.

Examples

Configure the hold time of a statistics group as 3 minutes.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] statistics hold-time 3
```

statistics max-group

Syntax

statistics max-group *number*

undo statistics max-group

View

DLSw, DNS, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice operation view

Default level

2: System level

Parameters

number: Specifies the maximum number of statistics groups that can be kept, in the range of 0 to 100. To disable collecting statistics, specify number 0.

Description

Use **statistics max-group** to configure the maximum number of statistics groups that can be kept.

Use **undo statistics max-group** to restore the default.

By default, 2 statistics groups at most can be kept.

When the number of statistics groups kept reaches the upper limit and a new statistics group is to be saved, the earliest statistics group is deleted.

This command is not supported by DHCP tests.

Examples

Configure the NQA to save up to 5 statistics groups for the ICMP test group.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] statistics max-group 5
```

statistics interval

Syntax

statistics interval *interval*

undo statistics interval

View

DLSw, DNS, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice operation view

Default level

2: System level

Parameters

interval: Specifies the interval in minutes for collecting statistics of the test results for a test group, in the range of 1 to 35791394.

Description

Use **statistics interval** to configure the interval for collecting test result statistics for a test group.

Use **undo statistics interval** to restore the default.

By default, the interval is 60 minutes.

NQA groups tests completed in the specified interval, and calculates the test result statistics. The statistics form a statistics group. To view information about the statistics groups, use the **display nqa statistics** command.

This command is not supported by DHCP tests.

Examples

Configure the interval for collecting the test result statistics of an ICMP test group as 2 minutes.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] statistics interval 2
```

tos

Syntax

tos *value*

undo tos

View

DLSw, DNS, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice, DHCP operation view

Default level

2: System level

Parameters

value: Specifies the value of the ToS (Type of Service) field in the IP header in an NQA probe packet, in the range of 0 to 255.

Description

Use **tos** to configure the value of the ToS field in the IP header in an NQA probe packet.

Use **undo tos** to restore the default.

By default, the ToS field in the IP header of an NQA probe packet is 0.

Examples

Configure the ToS field in an IP packet header in an NQA probe packet as 1.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] tos 1
```

ttl

Syntax

ttl *value*

undo ttl

View

DLSw, DNS, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice operation view

Default level

2: System level

Parameters

value: Specifies the maximum number of hops that a probe packet traverses in the network, in the range of 1 to 255.

Description

Use **ttl** to configure the maximum number of hops that a probe packet traverses in the network.

Use **undo ttl** to restore the default.

By default, the maximum number of hops that a probe packet can traverse in a network is 20.

After you configure the **route-option bypass-route** command, the maximum number of hops that a probe packet traverses in the network is 1, and the **ttl** command does not take effect.

Examples

Configure the maximum number of hops that a probe packet can traverse in a network as 16.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] ttl 16
```

type

Syntax

type { dhcp | dlsw | dns | ftp | http | icmp-echo | snmp | tcp | udp-echo | udp-jitter | voice }

View

NQA test group view

Default level

2: System level

Parameters

dhcp: Specifies a DHCP test.

dlsw: Specifies a DLSw test.

dns: Specifies a DNS test.

ftp: Specifies an FTP test.

http: Specifies an HTTP test.

icmp-echo: Specifies an ICMP echo test.

snmp: Specifies an SNMP test.

tcp: Specifies a TCP test.

udp-echo: Specifies a UDP echo test.

udp-jitter: Specifies a UDP jitter test.

voice: Specifies a voice test.

Description

Use **type** to configure the test type of the current test group and enter operation view.

By default, no test type is configured.

Examples

```
# Configure the test type of a test group as FTP and enter operation view.
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp]
```

url

Syntax

```
url url
undo url
```

View

HTTP operation view

Default level

2: System level

Parameters

url: Specifies the website that an HTTP test visits, a case-sensitive string of 1 to 185 characters.

Description

Use **url** to configure the website that an HTTP test visits.

Use **undo url** to remove the configured website that an HTTP test visits.

The character string of the configured URL cannot contain spaces.

Examples

```
# Configure the website that an HTTP test visits as /index.htm.
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type http
[Sysname-nqa-admin-test-http] url /index.htm
```

username (FTP operation view)

Syntax

```
username username
undo username
```

View

FTP operation view

Default level

2: System level

Parameters

username: Specifies the username that is used to log in to the FTP server. The username takes a case-sensitive string of 1 to 32 characters.

Description

Use **username** to configure a username used to log onto the FTP server.

Use **undo username** to remove the configured username.

By default, no username is configured for logging onto the FTP server.

Related commands: **password** and **operation**.

Examples

Configure the login username as **administrator**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] username administrator
```

NQA server configuration commands



IMPORTANT:

You only need to configure the NQA server for UDP jitter, TCP, UDP echo and voice tests.

display nqa server status

Syntax

display nqa server 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 nqa server status** to display NQA server status.

Examples

Display NQA server status.

```
<Sysname> display nqa server status
nqa server is: enabled
tcp-connect:
      IP Address      Port      Status
```


2.2.2.2	2000	active
udp-echo:		
IP Address	Port	Status
3.3.3.3	3000	inactive

Table 37 Command output

Field	Description
tcp-connect	NQA server status in the NQA TCP test.
udp-echo	NQA server status in the NQA UDP test.
IP Address	IP address specified for the TCP/UDP listening service on the NQA server.
Port	Port number of the TCP/UDP listening service on the NQA server.
Status	Listening service status, which can be one of the following values: <ul style="list-style-type: none"> active—Listening service is ready. inactive—Listening service is not ready.

nqa server enable

Syntax

nqa server enable
undo nqa server enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **nqa server enable** to enable the NQA server.

Use **undo nqa server enable** to disable the NQA server.

By default, the NQA server is disabled.

Related commands: **nqa server tcp-connect**, **nqa server udp-echo**, and **display nqa server status**.

Examples

```
# Enable the NQA server.
<Sysname> system-view
[Sysname] nqa server enable
```

nqa server tcp-connect

Syntax

nqa server tcp-connect *ip-address port-number*

undo nqa server tcp-connect *ip-address port-number*

View

System view

Default level

2: System level

Parameters

ip-address: Specifies the IP address specified for the TCP listening service on the NQA server.

port-number: Specifies the port number specified for the TCP listening service on the NQA server, in the range of 1 to 50000.

Description

Use **nqa server tcp-connect** to create a TCP listening service on the NQA server.

Use **undo nqa server tcp-connect** to remove the TCP listening service created.

Configure the command on the NQA server for TCP tests only.

The IP address and port number must be consistent with those on the NQA client and must be different from those for an existing listening service.

The IP address must be that of an interface on the NQA server. Otherwise, the configuration will be invalid.

Related commands: **nqa server enable** and **display nqa server status**.

Examples

Create a TCP listening service by using the IP address 169.254.10.2 and port 9000.

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

```
[Sysname] nqa server tcp-connect 169.254.10.2 9000
```

nqa server tcp-connect tos

Syntax

nqa server tcp-connect tos *tos*

undo nqa server tcp-connect tos

View

System view

Default level

2: System level

Parameters

tos: Specifies the value of the ToS field, in the range of 0 to 255.

Description

Use **nqa server tcp-connect tos** to configure the ToS value in the packets sent by TCP listening service on the NQA server.

Use **undo nqa server tcp-connect tos** to restore the default value.

By default, the ToS value is 0.

Examples

```
# Set the ToS value to 30 in the packets sent by the TCP listening service on the NQA server,
<Sysname> system-view
[Sysname] nqa server tcp-connect tos 30
```

nqa server udp-echo

Syntax

```
nqa server udp-echo ip-address port-number
undo nqa server udp-echo ip-address port-number
```

View

System view

Default level

2: System level

Parameters

ip-address: Specifies the IP address specified for the UDP listening service on the NQA server.

port-number: Specifies the port number specified for the UDP listening service on the NQA server, in the range of 1 to 50000.

Description

Use **nqa server udp-echo** to create a UDP listening service on the NQA server.

Use **undo nqa server udp-echo** to remove the UDP listening service created.

Configure the command on the NQA server for UDP jitter, UDP echo and voice tests only.

The IP address and port number must be consistent with those configured on the NQA client and must be different from those of an existing listening service.

The IP address must be that of an interface on the NQA server. Otherwise, the configuration becomes invalid.

Related commands: **nqa server enable** and **display nqa server status**.

Examples

```
# Create a UDP listening service by using the IP address 169.254.10.2 and port 9000.
<Sysname> system-view
[Sysname] nqa server udp-echo 169.254.10.2 9000
```

nqa server udp-echo tos

Syntax

```
nqa server udp-echo tos tos
undo nqa server udp-echo tos
```

View

System level

Default level

2: System level

Parameters

tos: Specifies the value of the ToS field, in the range of 0 to 255.

Description

Use **nqa server udp-echo tos** to configure the ToS value in the packets sent by the UDP listening service on the NQA server.

Use **undo nqa server udp-echo tos** to restore the default value.

By default, the ToS value is 0.

Examples

Set the ToS value to 30 in the packets sent by the UDP listening service enabled on the NQA server.

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

```
[Sysname] nqa server udp-echo tos 30
```

sFlow configuration commands

display sflow

Syntax

display sflow [**slot** *slot-number*] [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

2: System level

Parameters

slot *slot-number*: Displays the sFlow configuration and operation information of an IRF member switch. The *slot-number* argument specifies the ID of the IRF member switch.

|: 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 sflow** to display the sFlow configuration and operation information.

Examples

Display the sFlow configuration and operation information.

```
<Sysname> display sflow
```

```
sFlow Version: 5
```

```
sFlow Global Information:
```

```
Agent          IP:10.10.10.1 (Auto)
```

```
Source  Address:10.0.0.1 2001::1
```

```
Collector Information
```

ID	IP	Port	Aging	Size	Description
1	22:2:20::10	6535	N/A	3000	netserver
2	192.168.3.5	6543	500	3000	Office
3		6343	0	1400	
4		6343	0	1400	
5		6343	0	1400	
6		6343	0	1400	
7		6343	0	1400	
8		6343	0	1400	
9		6343	0	1400	
10		6343	0	1400	

sFlow Port Information:

Interface	CID	Interval(s)	FID	MaxHLen	Rate	Mode	Status
GE1/0/1	1	100	1	128	1000	Random	Active
GE1/0/2	2	100	2	128	1000	Random	Active

Table 38 Command output

Field	Description
sFlow Version	Current sFlow version. 5 —sFlow version 5.
sFlow Global Information	sFlow global configuration information.
Agent	IP address of the sFlow agent: <ul style="list-style-type: none"> • CLI—Manually configured IP address. • Auto—Automatically obtained IP address.
Source Address	Source IP address of sent sFlow packets.
Collector Information	sFlow collector information.
ID	sFlow collector ID.
IP	IP address of the sFlow collector that receives sFlow packets.
Port	Number of the port receiving sFlow packets on the sFlow collector.
Aging	Remaining lifetime of the sFlow collector. If N/A is displayed, the sFlow collector is never aged out.
Size	Maximum length of the sFlow data portion in an sFlow packet.
Description	Description of the sFlow collector.
sFlow Port Information	Information of the sFlow enabled ports.
Interface	sFlow enabled interface.
CID	ID of the target collector, for receiving the counter sampling data.
Interval(s)	Counter sampling interval, in seconds.
FID	ID of the target collector, for receiving the flow sampling data.
MaxHLen	Maximum copied length of a sampled packet.
Rate	Packet sampling interval.
Mode	Packet sampling mode, which can only be random and samples a random number of packets.
Status	Status of the sFlow enabled port: <ul style="list-style-type: none"> • Suspend—Indicates the port is down. • Active—Indicates the port is up.

sflow agent

Syntax

sflow agent { **ip** *ip-address* | **ipv6** *ipv6-address* }

undo sflow agent { **ip** | **ipv6** }

View

System view

Default level

2: System level

Parameters

ip *ip-address*: Specifies the IPv4 address of the sFlow agent.

ipv6 *ipv6-address*: Specifies the IPv6 address of the sFlow agent.

Description

Use **sflow agent** to configure the IP address of the sFlow agent.

Use **undo sflow agent** to remove the configured IP address.

By default, no IP address is configured for the sFlow agent. The device periodically checks the existence of sFlow agent address. If the sFlow agent has no IP address configured, the device automatically selects an interface IP address for the sFlow agent but does not save the selected IP address.

NOTE:

- HP recommends that you configure an IP address manually for the sFlow agent.
 - Only one IP address can be specified for the sFlow agent on the switch.
-

Examples

Configure the IP address of the sFlow agent.

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

```
[Sysname] sflow agent ip 10.10.10.1
```

sflow collector

Syntax

sflow collector *collector-id* { { **ip** *ip-address* | **ipv6** *ipv6-address* } | **datagram-size** *size* | **description** *text* | **port** *port-number* | **time-out** *seconds* } *

undo sflow collector *collector-id*

View

System view

Default level

2: System level

Parameters

collector-id: Specifies the ID of the sFlow collector. The switch can support ten sFlow collectors.

ip *ip-address*: Specifies the IPv4 address of the sFlow collector.

ipv6 *ipv6-address*: Specifies the IPv6 address of the sFlow collector.

description *text*: Specifies a description for the sFlow collector. The default description is "CLI Collector."

datagram-size *size*: Specifies the maximum length of the sFlow data portion in every sFlow packet that is sent out. The value ranges from 200 to 3000 bytes and defaults to 1400 bytes.

port *port-number*: Specifies the port number of the sFlow collector, in the range of 1 to 65535. The default port number is 6343.

time-out *seconds*: Specifies the aging time of the sFlow collector, in the range of 60 to 2147483647, in seconds. By default, the sFlow collector never ages out. When the aging time expires, all the settings of the sFlow collector are restored to the default. The system does not save the configuration of collectors with an aging time specified.

Description

Use **sflow collector** to configure an sFlow collector.

Use **undo sflow collector** to remove a specified sFlow collector.

By default, the device provides a number of sFlow collectors. You can use the **display sflow** command to display these sFlow collectors.

Examples

```
# Specify sFlow collector 2's destination IP address as 3.3.3.1, port number as default, description as
netserver, aging time as 1200 seconds, and maximum length of the sFlow data portion as 1000 bytes.
<Sysname> system-view
[Sysname] sflow collector 2 ip 3.3.3.1 description netserver time-out 1200 datagram-size
1000
```

sflow counter interval

Syntax

sflow counter interval *interval-time*

undo sflow counter interval

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

interval-time: Specifies the counter sampling interval in seconds, in the range of 2 to 86400.

Description

Use **sflow counter interval** to set the counter sampling interval.

Use **undo sflow counter interval** to disable sFlow counter sampling.

By default, counter sampling is disabled.

This command is supported only on physical Ethernet interfaces, but not on logical interfaces (such as VLAN interfaces).

Examples

```
# Set the counter sampling interval to 120 seconds on GigabitEthernet 1/0/1.
<Sysname> system-view
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] sflow counter interval 120
```


sflow counter collector

Syntax

sflow counter collector *collector-id*

undo sflow counter collector

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

collector-id: Specifies the ID of the sFlow collector.

Description

Use **sflow counter collector** to specify the sFlow collector for counter sampling.

Use **undo sflow counter collector** to remove the sFlow collector for counter sampling.

By default, no sFlow collector is specified for counter sampling.

This command is supported only on physical Ethernet interfaces, but not on logical interfaces (such as VLAN interfaces).

Examples

Specify sFlow collector 2 on GigabitEthernet 1/0/1 for counter sampling.

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

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] sflow counter collector 2
```

sflow flow collector

Syntax

sflow flow collector *collector-id*

undo sflow flow collector

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

collector-id: Specifies the ID of the sFlow collector.

Description

Use **sflow flow collector** to specify the sFlow collector for flow sampling.

Use **undo sflow flow collector** to remove the sFlow collector configured for flow sampling.

By default, no sFlow collector is specified for flow sampling.

This command is supported only on physical Ethernet interfaces, but not on logical interfaces (such as VLAN interfaces).

Examples

```
# Specify the collector number 2 on GigabitEthernet 1/0/1 for flow sampling.
<Sysname> system-view
[Sysname] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] sflow flow collector 2
```

sflow flow max-header

Syntax

```
sflow flow max-header length
undo sflow flow max-header
```

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

Length: Specifies the maximum bytes of a sampled packet that can be copied, in the range of 18 to 512.

Description

Use **sflow flow max-header** to set the maximum bytes of a sampled packet that can be copied (starting from the header).

Use **undo sflow flow max-header** to restore the default.

By default, up to 128 bytes of a sampled packet that can be copied. HP recommends you use the default value.

This command is supported only on physical Ethernet interfaces, but not on logical interfaces (such as VLAN interfaces).

Examples

```
# Set the maximum bytes of a sampled packet that can be copied to 60.
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] sflow flow max-header 60
```

sflow sampling-mode

Syntax

```
sflow sampling-mode { determine | random }
undo sflow sampling-mode
```

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

determine: Specifies the fixed sampling mode. For example, if the flow sampling interval is set to 4000 (by using the **sflow sampling-rate** command), the device randomly samples a packet, like the tenth packet, from the first 4000 packets. The next time the device samples the 4010th packet, and so on.

random: Specifies the random sampling mode. After the sampling interval is specified with the **sflow sampling-rate** command, a device samples zero, one, or multiple packets from each group of sampled packets. Generally, one packet is sampled from each group of sampled packets. For example, with the packet sampling rate set to 4000, the device may sample one packet from the first 4000 packets, two from the next 4000 packets, and none from the third 4000 packets, but generally the device samples one packet from 4000 packets.

Description

Use **sflow sampling-mode** to specify the packet sampling mode.

Use **undo sflow sampling-mode** to restore the default.

The default mode is **random**.

This command is supported only on physical Ethernet interfaces, but not on logical interfaces (such as VLAN interfaces).

Related commands: **sflow sampling-rate**.

NOTE:

The switch does not support the flow sampling mode **determine**.

Examples

Specify the random sample mode on GigabitEthernet 1/0/1.

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

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] sflow sampling-mode random
```

sflow sampling-rate

Syntax

sflow sampling-rate *interval*

undo sflow sampling-rate

View

Layer 2 Ethernet interface view

Default level

2: System level

Parameters

interval: Specifies the number of packets out of which the interface will sample a packet, ranging from 1000 to 500000.

Description

Use **sflow sampling-rate** to specify the number of packets out of which the interface will sample a packet.

Use **undo sflow sampling-rate** to disable sampling.

By default, packet sampling is disabled.

This command is supported only on Ethernet interfaces, but not on logical interfaces (such as VLAN interfaces).

The bigger the value of the *interval* argument, the lower the sampling rate, and vice versa.

Related commands: **sflow sampling-mode**.

Examples

Set GigabitEthernet 1/0/1 to sample a packet out of 4000 packets.

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

```
[Sysname] interface GigabitEthernet1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] sflow sampling-rate 4000
```

sflow source

Syntax

sflow source { **ip** *ip-address* | **ipv6** *ipv6-address* } *

undo sflow source { **ip** | **ipv6** } *

View

System view

Default level

2: System level

Parameters

ip *ip-address*: Specifies the source IPv4 address of sent sFlow packets.

ipv6 *ipv6-address*: Specifies the source IPv6 address of sent sFlow packets.

Description

Use **sflow source** to specify the source IP address of sent sFlow packets.

Use **undo sflow source** to remove the specified source IP address.

By default, no source IP address is specified for sent sFlow packets.

Examples

Specify the source IPv4 address of sent sFlow packets as 10.0.0.1.

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

```
[Sysname] sflow source ip 10.0.0.1
```

IPC configuration commands

The **display** commands for the IPC feature display only information about active nodes.

display ipc channel

Syntax

```
display ipc channel { node node-id | self-node } [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

node *node-id*: Displays channel information for a node. The *node-id* argument takes a node number in the range of 0 to 10.

self-node: Displays channel information for the local node.

|: 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 ipc channel** to display channel information for a node.

Examples

```
# Display channel information for node 1.
<Sysname> display ipc channel node 1
ChannelID      Description
-----
19             RPC channel
72             Portal Backup Channel
79             DHCP
94             IPC test channel
149            Prehistorical channel, NO.1
```

Table 39 Command output

Field	Description
ChannelID	Channel number, which has been predefined and assigned by the system. One channel number corresponds to one module. The display ipc channel command displays the numbers of the current active modules.
Description	Description information, which is generated by the internal software of the device, is used to describe the functions of a channel. For example, "FIB4" indicates that the channel is used for Layer 3 fast forwarding. "Prehistorical channel, NO.2" indicates that no description is defined for the channel, and the channel is the second channel established.

display ipc link

Syntax

```
display ipc link { node node-id | self-node } [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

node node-id: Displays the link status of the specified node, where *node-id* represents the number of the specified node. The value is in the range of 0 to 10.

self-node: Displays the link status of the local node.

|: 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 ipc link** to display the link status of the specified node.

Examples

```
# Display link status information for the local node.
```

```
<Sysname> display ipc link self-node
```

```
Dst-NodeID      LinkStatus
```

```
-----
```

```
1                UP
```

```
2                DOWN
```

The output shows that:

- An UP connection exists between the local node and node 1.
- A DOWN connection exists between the local node and node 2.

Table 40 Command output

Field	Description
DstNodeID	Number of the peer node.
LinkStatus	Link status: <ul style="list-style-type: none"> • UP—A connection is established. • DOWN—A connection is terminated.

display ipc multicast-group

Syntax

```
display ipc multicast-group { node node-id | self-node } [ | { begin | exclude | include }
regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

node node-id: Displays the multicast group information for the specified node, where *node-id* represents the number of the specified node. The value is in the range of 0 to 10.

self-node: Displays the multicast group information for the local node.

|: 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 ipc multicast-group** to display multicast group information for the specified node.

Examples

```
# Display multicast group information for node 1.
<Sysname> display ipc multicast-group node 1
GroupID      Status      ChannelID
-----
8             INUSE         12
```

Table 41 Command output

Field	Description
GroupID	Multicast group ID.

Field	Description
Status	Link status: <ul style="list-style-type: none"> • INUSE—The multicast group is in use. • DELETE—The multicast group is to be deleted.
ChannelID	Channel number.

display ipc node

Syntax

display ipc node [[{ **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 ipc node** to display node information.

Examples

Display node information for the device.

```
<Sysname> display ipc node
Self node ID: 1
Current active node ID: 1
```

Table 42 Command output

Field	Description
Self node ID	Number of the local node
Current active node ID	List of the current active nodes

display ipc packet

Syntax

display ipc packet { **node** *node-id* | **self-node** } [[{ **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

node *node-id*: Displays the packet statistics for the specified node, where *node-id* represents the number of the specified node. The value is in the range of 0 to 10.

self-node: Displays the packet statistics for the local node.

|: 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 ipc packet** to display the packet statistics for the specified node.

Examples

Display the packet statistics for the local node.

```
<Sysname> display ipc packet self-node
```

```
ChannelID Sent-fragments Sent-packets Received-fragments Received-packets
```

```
-----  
11          828           810           819           810  
13           0           0           0           0  
14           5           3           5           5  
15           0           0           0           0  
16           0           0           0           0  
17          50          50          37          35  
19           0           0           0           0
```

Table 43 Command output

Field	Description
ChannelID	Channel number.
Sent-fragments	Number of fragments sent.
Sent-packets	Number of packets sent. Whether a packet is fragmented depends on the interface MTU and the packet size in bytes. If the packet size is larger than the MTU, the packet is fragmented. If the packet size is smaller than or equal to the MTU, the packet is sent.
Received-fragments	Number of fragments successfully received.
Received-packets	Number of packets successfully received. If fragments are received on an interface, the system reassembles the fragments and sends a complete packet to the upper layer.

display ipc performance

Syntax

```
display ipc performance { node node-id | self-node } [ channel channel-id ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

node *node-id*: Displays the IPC performance statistics for the specified node, where *node-id* represents the number of the specified node. The value is in the range of 0 to 10.

self-node: Displays the IPC performance statistics for the local node.

channel *channel-id*: Displays the IPC performance statistics for the specified channel, where *channel-id* represents the channel number. The value range depends on the switch model.

|: 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 ipc performance** to display IPC performance statistics.

If IPC performance statistics is enabled, the command displays the current IPC performance statistics. If IPC performance statistics is disabled, the command displays the IPC performance statistics collected before IPC performance statistics was disabled.

Related commands: **ipc performance enable**.

Examples

Display the IPC performance statistics for node 1.

```
<Sysname> display ipc performance node 1
```

Peak: Peak rate (pps)

10Sec: Average rate in the last 10 seconds (pps)

1Min: Average rate in the last 1 minute (pps)

5Min: Average rate in the last 5 minutes (pps)

Total-Data: Total number of data (packets)

Statistics for packets sent successfully:

Peak	10Sec	1Min	5Min	Total-Data
1	1	1	0	80

Statistics for packets recieved successfully:

Peak	10Sec	1Min	5Min	Total-Data
------	-------	------	------	------------

1	1	1	0	82
Statistics for packets acknowledged:				
Peak	10Sec	1Min	5Min	Total-Data
1	1	1	0	78

Table 44 Command output

Field	Description
Peak	Peak rate in pps (average rate is measured every 10 seconds, the greatest value of which is taken as the peak rate).
10Sec	Average rate (in pps) for the past 10 seconds.
1Min	Average rate (in pps) for the past 1 minute.
5Min	Average rate (in pps) for the past 5 minutes.
Total-Data	Total amount of data collected from the time when IPC performance statistics was enabled to the time when this command was executed.

display ipc queue

Syntax

display ipc queue { **node** *node-id* | **self-node** } [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

node *node-id*: Displays sending queue information for the specified node, where *node-id* represents the number of the specified node. The value is in the range of 0 to 10.

self-node: Displays sending queue information for the local node.

|: 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 ipc queue** to display sending queue information for the specified node.

Examples

Display sending queue information for the local node.

```
<Sysname> display ipc queue self-node
```

```
QueueType QueueID Dst-NodeID Length FullTimes Packet
```

UNICAST	0	0	4096	0	0
UNICAST	1	0	4096	0	0
UNICAST	2	0	4096	0	0
UNICAST	3	0	4096	0	0
UNICAST	0	1	4096	0	0
UNICAST	1	1	4096	0	0
UNICAST	2	1	4096	0	0
UNICAST	3	1	4096	0	0
MULTICAST	0	--	4096	0	0
MULTICAST	1	--	4096	0	0
MULTICAST	2	--	512	0	0
MULTICAST	3	--	512	0	0
MULTICAST	4	--	512	0	0
MULTICAST	5	--	512	0	0
MIXCAST	0	--	2048	0	0
MIXCAST	1	--	2048	0	0

Table 45 Command output

Field	Description
QueueType	Queue type: <ul style="list-style-type: none"> UNICAST—Unicast queue. MULTICAST—Multicast (including broadcast) queue. MIXCAST—Mixcast queue, which can accommodate unicasts, multicasts, and broadcasts.
QueueID	Queue number.
DstNodeID	Peer node number. If no peer node exists, two hyphens (-) are displayed.
Length	Queue length (number of packets that can be buffered).
FullTimes	Number of times the queue was full.
Packet	Total number of packets in the queue.

ipc performance enable

Syntax

```
ipc performance enable { node node-id | self-node } [ channel channel-id ]
undo ipc performance enable [ node node-id | self-node ] [ channel channel-id ]
```

View

User view

Default level

1: Monitor level

Parameters

node *node-id*: Enables IPC performance statistics for the specified node, where *node-id* represents the number of the specified node. The value is in the range of 0 to 10.

self-node: Enables IPC performance statistics for the local node.

channel *channel-id*: Enables IPC performance statistics for the specified channel, where *channel-id* represents the channel number. The value range depends on the switch model.

Description

Use **ipc performance enable** to enable IPC performance statistics. Use the **undo ipc performance** command to disable IPC performance statistics.

By default, IPC performance statistics is disabled.

When IPC performance statistics is disabled, the statistics data does not change. The **display ipc performance** command displays the statistics collected before IPC performance statistics was disabled.

Examples

Enable IPC performance statistics of channel **18** on node **1**.

```
<Sysname> ipc performance enable node 1 channel 18
```

reset ipc performance

Syntax

reset ipc performance [**node** *node-id* | **self-node**] [**channel** *channel-id*]

View

User view

Default level

1: Monitor level

Parameters

node *node-id*: Clears the IPC performance statistics for the specified node, where *node-id* represents the number of the specified node. The value is in the range of 0 to 10.

self-node: Clears the IPC performance statistics for the local node.

channel *channel-id*: Clears the IPC performance statistics for the specified channel, where *channel-id* represents the channel number. The value range depends on the switch model.

Description

Use **reset ipc performance** to clear IPC performance statistics.

Examples

Clear the IPC performance statistics of channel 18 on node 1.

```
<Sysname> reset ipc performance node 1 channel 18
```

PoE configuration commands

apply poe-profile

Syntax

```
apply poe-profile { index index | name profile-name }  
undo apply poe-profile { index index | name profile-name }
```

View

PoE interface view

Default level

2: System level

Parameters

index *index*: Specifies a PoE profile by its index number in the range of 1 to 100.

name *profile-name*: Specifies a PoE profile by its name, a string of 1 to 15 characters.

Description

Use **apply poe-profile** to apply a PoE profile to a PoE interface.

Use **undo apply poe-profile** to remove a PoE profile from a PoE interface.

The index number of the PoE profile is displayed when you execute the **display this** command.

Related commands: **display poe-profile** and **apply poe-profile interface**.

Examples

```
# Apply the PoE profile named forIPphone to PoE interface GigabitEthernet 1/0/20.  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/20  
[Sysname-GigabitEthernet1/0/20] apply poe-profile name forIPphone  
[Sysname-GigabitEthernet1/0/20] display this  
#  
interface GigabitEthernet1/0/20  
    apply poe-profile index 1  
#  
return
```

apply poe-profile interface

Syntax

```
apply poe-profile { index index | name profile-name } interface interface-range  
undo apply poe-profile { index index | name profile-name } interface interface-range
```

View

System view

Default level

2: System level

Parameters

index *index*: Specifies a PoE profile by its index number, in the range of 1 to 100.

name *profile-name*: Specifies a PoE profile by its name, a string of 1 to 15 characters.

interface-range: Specifies a range of Ethernet interfaces in the form of *interface-type interface-number* [**to** *interface-type interface-number*], where *interface-type interface-number* represents the interface type and interface number. The start interface number must be smaller than the end interface number. If an interface in the specified range does not support PoE, it is ignored when the PoE profile is applied.

Description

Use **apply poe-profile interface** to apply a PoE profile to a range of PoE interfaces.

Use **undo apply poe-profile interface** to remove a PoE profile from a range of PoE interfaces.

Related commands: **display poe-profile interface** and **apply poe-profile**.

Examples

Apply the PoE profile named **forIPphone** to PoE interface GigabitEthernet 1/0/1.

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

```
[Sysname] apply poe-profile name forIPphone interface gigabitethernet 1/0/1
```

Apply the PoE profile with index number 1 to PoE interfaces GigabitEthernet 1/0/2 through GigabitEthernet 1/0/8.

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

```
[Sysname] apply poe-profile index 1 interface gigabitethernet 1/0/2 to gigabitethernet 1/0/8
```

display poe device

Syntax

display poe device [| { **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 poe device** to display brief PSE information, including the ID, slot number, and state of PSEs.

Examples

Display PSE information. The output depends on the device model.

```
<Sysname> display poe device
```

PSE ID	SlotNo	SubSNo	PortNum	MaxPower(W)	State	Model
4	1	0	24	370	off	PD67024

Table 46 Command output

Field	Description
PSE ID	ID of the PSE.
SlotNo	Slot number of the PSE.
SubSNo	Sub-slot number of the PSE.
PortNum	Number of PoE interfaces on the PSE.
MaxPower(W)	Maximum power of the PSE.
State	PSE state: <ul style="list-style-type: none">• on—The PSE is supplying power.• off—The PSE stops supplying power.• faulty—The PSE fails.
Model	PSE model.

display poe interface

Syntax

```
display poe 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 *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 poe interface** to display power supplying information for PoE interfaces.

If no interface is specified, this command displays power supplying information for all PoE interfaces.

Examples

Display power supplying information for GigabitEthernet 1/0/1.

```
<Sysname> display poe interface gigabitethernet 1/0/1
Port Power Enabled           : enabled
Port Power Priority          : high
Port Operating Status       : on
Port IEEE Class             : 0
Port Detection Status       : delivering-power
Port Power Mode             : signal
Port Current Power          : 3600      mW
Port Average Power          : 3662      mW
Port Peak Power             : 3900      mW
Port Max Power              : 15400     mW
Port Current                : 71        mA
Port Voltage                : 50.9      V
Port PD Description         : IP Phone For Room 101
```

Table 47 Command output

Field	Description
Port Power Enabled	PoE state: <ul style="list-style-type: none"> enabled. disabled.
Port Power Priority	Power priority of the PoE interface: <ul style="list-style-type: none"> critical (highest). high. low.
Port Operating Status	Operating state of a PoE interface: <ul style="list-style-type: none"> off—PoE is disabled. on—Power is supplied for a PoE interface normally. power-lack—Guaranteed remaining power of the PSE is not high enough to supply power for a critical PoE interface. power-deny—PSE refuses to supply power. The power required by the powered device (PD) is higher than the configured power. power-itself—External equipment is supplying power for itself. power-limit—PSE is supplying a limited power. The power required by the PD is higher than the configured power and the PSE still supplies the configured power.
Port IEEE class	PD power class: 0, 1, 2, 3, or 4. If PoE is not supported, this field displays a hyphen (-).
Port Detection Status	Power detection state of a PoE interface: <ul style="list-style-type: none"> disabled—PoE function is disabled. searching—PoE interface is searching for the PD. delivering-power—PoE interface is supplying power for the PD. fault—There is a fault defined in 802.3af. test—PoE interface is under test. other-fault—There is a fault other than defined in 802.3af. pd-disconnect—PD is disconnected.

Field	Description
Port Power Mode	Power mode of a PoE interface. signal indicates that power is supplied over signal cables.
Port Current Power	Current power of a PoE interface, including PD consumption power and transmission loss. Transmission loss usually does not exceed one watt.
Port Average Power	Average power of a PoE interface.
Port Peak Power	Peak power of a PoE interface.
Port Max Power	Maximum power of a PoE interface.
Port Current	Current of a PoE interface.
Port Voltage	Voltage of a PoE interface.
Port PD Description	Description of the PD connected to the PoE interface, which is used to identify the type and location of the PD.

Display power supplying information for all PoE interfaces.

```
<Sysname> display poe interface
```

```

Interface  Status  Priority  CurPower  Operating  IEEE  Detection
              (W)              Status      Class  Status
GE1/0/1    enabled high    3.6      on        0      delivering-power
GE1/0/2    enabled low    0.0      off       0      searching
GE1/0/3    enabled low    0.0      off       0      searching
GE1/0/4    enabled low    0.0      off       0      searching
GE1/0/5    enabled low    0.0      off       0      searching
GE1/0/6    enabled low    0.0      off       0      searching
GE1/0/7    enabled low    0.0      off       0      searching
GE1/0/8    enabled low    0.0      off       0      searching
.....
GE1/0/23   enabled low    0.0      off       0      searching
GE1/0/24   enabled low    0.0      off       0      searching

--- 1 port(s) on,    3.6 (W) consumed,    367.4 (W) remaining ---
```

Table 48 Command output

Field	Description
Interface	Shortened form of a PoE interface.
Enable	PoE state: <ul style="list-style-type: none"> enabled. disabled.
Priority	Power priority of a PoE interface: <ul style="list-style-type: none"> critical (highest). high. low.
CurPower	Current power of a PoE interface.

Field	Description
Operating Status	<p>Operating state of a PoE interface:</p> <ul style="list-style-type: none"> • off—PoE is disabled. • on—Power is supplied for a PoE interface normally. • power-lack—Guaranteed remaining power of the PSE is not high enough to supply power for a critical PoE interface. • power-deny—PSE refuses to supply power. The power required by the powered device (PD) is higher than the configured power. • power-itself—External equipment is supplying power for itself. • power-limit—PSE is supplying a limited power. The power required by the PD is higher than the configured power and the PSE still supplies the configured power.
IEEE class	PD power class defined by IEEE.
Detection Status	<p>Power detection state of a PoE interface:</p> <ul style="list-style-type: none"> • disabled—PoE function is disabled. • searching—PoE interface is searching for the PD. • delivering-power—PoE interface is supplying power for the PD. • fault—There is a fault defined in 802.3af. • test—PoE interface is under test. • other-fault—There is a fault other than defined in 802.3af. • pd-disconnect—PD is disconnected.
port(s) on	Number of PoE interfaces that are supplying power.
consumed	Power consumed by the current PoE interface.
Remaining	Remaining power that the PSE can still supply.

display poe interface power

Syntax

```
display poe interface power [ 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 *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 poe interface power** to display power information and settings for PoE interfaces.

If no interface is specified, this command displays power information for all PoE interfaces.

Examples

Display power information for GigabitEthernet 1/0/1.

```
<Sysname> display poe interface power GigabitEthernet 1/0/1
Interface    CurPower    PeakPower    MaxPower    PD Description
           (W)         (W)         (W)
GE1/0/1      0.0         0.0         30.0
```

Display power information for all PoE interfaces.

```
<Sysname> display poe interface power
Interface    CurPower    PeakPower    MaxPower    PD Description
           (W)         (W)         (W)
GE1/0/1      0.0         0.0         30.0
GE1/0/2      0.0         0.0         30.0
GE1/0/3      0.0         0.0         30.0
GE1/0/4      0.0         0.0         30.0
GE1/0/5      0.0         0.0         30.0
GE1/0/6      0.0         0.0         30.0
GE1/0/7      0.0         0.0         30.0
GE1/0/8      0.0         0.0         30.0
.....
GE1/0/23     0.0         0.0         30.0
GE1/0/24     0.0         0.0         30.0
--- 0 port(s) on,      0.0 (W) consumed,   370.0 (W) remaining ---
```

Table 49 Command output

Field	Description
Interface	Shortened form of a PoE interface.
CurPower	Current power of a PoE interface.
PeakPower	Peak power of a PoE interface.
MaxPower	Maximum power of a PoE interface.
PD Description	Description of the PD connected with a PoE interface. When the description contains more than 34 characters, the first 30 characters followed by four dots are displayed.
port(s) on	Number of PoE interfaces that are supplying power.
consumed	Power consumed by all PoE interfaces.
Remaining	Remaining power that the PSE can still supply.

display poe pse

Syntax

```
display poe pse [ pse-id ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

pse-id: Specifies a PSE by its ID. To view PSE ID and slot mappings, use the **display poe device** command. If no PSE is specified, this command displays information about all PSEs.

|: 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 poe pse** to display detailed PSE information, including its software version, hardware version, power settings, and power statistics.

Examples

Display detailed information about the PSE.

```
<Sysname> display poe pse
PSE ID                : 4
PSE Slot No           : 1
PSE SubSlot No        : 0
PSE Model              : PD67024
PSE Power Enabled      : enabled
PSE Power Priority      : -
PSE Current Power      : 0          W
PSE Average Power      : 0          W
PSE Peak Power         : 0          W
PSE Max Power          : 370        W
PSE Remaining Guaranteed : 370      W
PSE CPLD Version       : -
PSE Software Version   : 400
PSE Hardware Version   : 57603
PSE Legacy Detection    : disabled
PSE Utilization-threshold : 80
PSE Pd-policy Mode     : disable
PSE PD Disconnect Detect Mode : AC
```

Table 50 Command output

Field	Description
PSE Slot No	Member of the PSE.
PSE SubSlot No	Subslot number of the PSE.

Field	Description
PSE Model	Model of the PSE module.
PSE Power Enabled	PoE state, enabled or disabled.
PSE Power Priority	Power priority of the PSE.
PSE Current Power	Current power of the PSE.
PSE Average Power	Average power of the PSE.
PSE Peak Power	Peak power of the PSE.
PSE Max Power	Maximum power of the PSE.
PSE Remaining Guaranteed	Guaranteed remaining power of the PSE = Guaranteed maximum power of the PSE– the sum of the maximum power of the critical PoE interfaces of the PSE.
PSE CPLD Version	PSE CPLD version.
PSE Software Version	PSE software version number.
PSE Hardware Version	PSE hardware version number.
PSE Legacy Detection	Nonstandard PD detection by the PSE: <ul style="list-style-type: none"> • Enabled. • Disabled.
PSE Utilization-threshold	PSE power alarm threshold.
PSE Pd-policy Mode	PD power management policy mode.
PSE PD Disconnect Detect Mode	PD disconnection detection mode.

display poe pse interface

Syntax

```
display poe pse pse-id interface [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

pse *pse-id*: Specifies a PSE ID. To display PSE ID and slot mappings, use the **display poe device** command.

|: 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 poe pse interface** to display the PoE state of all PoE interfaces connected to a PSE.

Examples

Display the power state of all PoE interfaces connected to PSE 4.

```
<Sysname> display poe pse 4 interface
Interface      Status      Priority CurPower Operating IEEE      Detection
              (W)          Status    Class    Status
GE1/0/1        disabled low         0.0      off      0        disabled
GE1/0/2        disabled low         0.0      off      0        disabled
GE1/0/3        disabled low         0.0      off      0        disabled
GE1/0/4        disabled low         0.0      off      0        disabled
GE1/0/5        disabled low         0.0      off      0        disabled
GE1/0/6        disabled low         0.0      off      0        disabled
GE1/0/7        disabled low         0.0      off      0        disabled
GE1/0/8        disabled low         0.0      off      0        disabled
.....
GE1/0/23       disabled low         0.0      off      0        disabled
GE1/0/24       disabled low         0.0      off      0        disabled
--- 0 port(s) on,    0.0 (W) consumed,   370.0 (W) remaining ---
```

Table 51 Command output

Field	Description
Interface	Shortened form of a PoE interface.
Status	PoE enabled/disabled state. For the value, see Table 47 .
Priority	Priority of a PoE interface. For the value, see Table 47 .
CurPower	Current power of a PoE interface.
Operating Status	Operating state of a PoE interface. For the value, see Table 47 .
IEEE Class	PD power class.
Detection Status	Power detection state of a PoE interface. For the value, see Table 47 .
port(s) on	Number of PoE interfaces that are supplying power.
consumed	Power consumed by PoE interfaces on the PSE.
Remaining	Remaining power that the PSE can still supply.

display poe pse interface power

Syntax

display poe pse *pse-id* **interface power** [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

pse *pse-id*: Specifies a PSE ID. To view the mapping between PSE ID and slot, use the **display poe device** command.

|: 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 poe pse interface power** to display power information for PoE interfaces connected with the PSE.

Examples

Display the power state of PoE interfaces connected with PSE 4.

```
<Sysname> display poe pse 4 interface power
Interface      CurPower    PeakPower    MaxPower    PD Description
              (W)         (W)          (W)
GE1/0/1        0.0         0.0          15.4
GE1/0/2        0.0         0.0          15.4
GE1/0/3        0.0         0.0          15.4
GE1/0/4        0.0         0.0          15.4
GE1/0/5        0.0         0.0          15.4
GE1/0/6        0.0         0.0          15.4
GE1/0/7        0.0         0.0          15.4
GE1/0/8        0.0         0.0          15.4
.....
GE1/0/23       0.0         0.0          15.4
GE1/0/24       0.0         0.0          15.4
--- 0 port(s) on,      0.0 (W) consumed,   370.0 (W) remaining ---
```

Table 52 Command output

Field	Description
Interface	Shortened form of a PoE interface.
CurPower	Current power of a PoE interface.
PeakPower	Peak power of a PoE interface.
MaxPower	Maximum power of a PoE interface.
PD Description	Description of the PD connected with a PoE interface. When the description contains more than 34 characters, the first 30 characters followed by four dots are displayed.
port(s) on	Number of PoE interfaces that are supplying power.
consumed	Power being consumed by all PoE interfaces.
Remaining	Remaining power that the PSE can still supply.

display poe-profile

Syntax

display poe-profile [**index** *index* | **name** *profile-name*] [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

index *index*: Specifies a PoE profile by its index number, in the range of 1 to 100.

name *profile-name*: Specifies a PoE profile by its name, a string of 1 to 15 characters.

|: 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 poe-profile** to display information about the PoE profile.

If no argument is specified, all information about the configurations and applications of existing PoE profiles is displayed.

Examples

Display information about all PoE profiles.

```
<Sysname> display poe-profile
Poe-profile   Index   ApplyNum  Interface  Configuration
forIPphone    1         6         GE1/0/5    poe enable
               GE1/0/6    poe priority critical
               GE1/0/7
               GE1/0/8
               GE1/0/9
               GE1/0/10
forAP          2         2         GE1/0/11    poe enable
               GE1/0/12    poe max-power 14000
---  2 poe-profile(s) created, 8 port(s) applied  ---
```

Display information about the PoE profile with index number 1.

```
<Sysname> display poe-profile index 1
Poe-profile   Index   ApplyNum  Interface  Configuration
forIPphone    1         6         GE1/0/5    poe enable
               GE1/0/6    poe priority critical
               GE1/0/7
               GE1/0/8
```

```

GE1/0/9
GE1/0/10

--- 6 port(s) applied ---

# Display information about PoE profile forIPphone.
<Sysname> display poe-profile name AA
Poe-profile      Index    ApplyNum  Interface  Configuration
forIPphone       1        6         GE1/0/5    poe enable
                  GE1/0/6    poe priority critical
                  GE1/0/7
                  GE1/0/8
                  GE1/0/9
                  GE1/0/10

--- 6 port(s) applied ---

```

Table 53 Command output

Field	Description
Poe-profile	Name of the PoE profile.
Index	Index number of the PoE profile.
ApplyNum	Number of PoE interfaces to which a PoE profile is applied.
Interface	Shortened form of the PoE interface to which the PoE configuration is applied.
Configuration	Configurations of the PoE profile.
poe-profile(s) created	Number of PoE profiles.
port(s) applied	Sum of the number of PoE interfaces to which all PoE profiles are respectively applied.

display poe-profile interface

Syntax

display poe-profile 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 *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 poe-profile interface** to display all information about the configurations and applications of the PoE profile that currently takes effect on the specified PoE interface.

Examples

Display all information about the configurations and applications of the current PoE profile applied to GigabitEthernet 1/0/1.

```
<Sysname> display poe-profile interface gigabitethernet 1/0/1
Poe-profile      Index   ApplyNum  Interface  Current Configuration
forIPphone       1       6         GE1/0/1    poe enable
                                     poe priority critical
```

Not all the configurations of a PoE profile can be applied successfully, so only the configurations that currently take effect on the interface are displayed. For the descriptions for other fields, see [Table 52](#).

poe disconnect

Syntax

poe disconnect { ac | dc }

undo poe disconnect

View

System view

Default level

2: System level

Parameters

ac: Specifies the PD disconnection detection mode as **ac**.

dc: Specifies the PD disconnection detection mode as **dc**.

Description

Use **poe disconnect** to configure a PD disconnection detection mode.

Use **undo poe disconnect** to restore the default.

The default PD disconnection detection mode is **ac**.

Changing to the PD disconnection detection mode may lead to power-off of some PDs.

Examples

Set the PD disconnection detection mode to **dc**.

```
<Sysname> system-view
[Sysname] poe disconnect dc
```

poe enable

Syntax

poe enable

undo poe enable

View

PoE interface view, PoE-profile file view

Default level

2: System level

Parameters

None

Description

Use **poe enable** to enable PoE on a PoE interface.

Use **undo poe enable** to disable PoE on a PoE interface.

By default, PoE is disabled on a PoE interface.

If a PoE profile is already applied to a PoE interface, remove the application of the file to the PoE interface before configuring the interface in PoE-profile view.

If a PoE profile is applied to a PoE interface, remove the application of the file to the PoE interface before configuring the interface in PoE interface view.

Examples

Enable PoE on a PoE interface.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe enable
```

Enable PoE on a PoE interface through a PoE profile.

```
<Sysname> system-view
[Sysname] poe-profile abc
[Sysname-poe-profile-abc-1] poe enable
[Sysname-poe-profile-abc-1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] apply poe-profile name abc
```

poe legacy enable

Syntax

poe legacy enable pse *pse-id*

undo poe legacy enable pse *pse-id*

View

System view

Default level

2: System level

Parameters

pse *pse-id*: Specifies a PSE ID.

Description

Use **poe legacy enable** to enable the PSE to detect nonstandard PDs.

Use **undo poe legacy enable** to disable the PSE from detecting nonstandard PDs.

By default, the PSE is disabled from detecting nonstandard PDs.

Examples

Enable PSE 7 to detect nonstandard PDs (for a device with multiple PSEs).

```
<Sysname> system-view
[Sysname] poe legacy enable pse 7
```

poe max-power

Syntax

poe max-power *max-power*

undo poe max-power

View

PoE interface view, PoE-profile file view

Default level

2: System level

Parameters

max-power: Specifies the maximum power in milliwatts allocated to a PoE interface. It is in the range of 1000 to 30000 milliwatts.

Description

Use **poe max-power** to configure the maximum power for a PoE interface.

Use **undo poe max-power** to restore the default.

By default, the maximum power that a PoE interface can supply is 30000 milliwatts.

Examples

Set the maximum power of GigabitEthernet 1/0/1 to 12000 milliwatts.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe max-power 12000
```

Set the maximum power of GigabitEthernet 1/0/1 to 12000 milliwatts in the PoE profile **abc**.

```
<Sysname> system-view
[Sysname] poe-profile abc
[Sysname-poe-profile-abc-1] poe max-power 12000
[Sysname-poe-profile-abc-1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] apply poe-profile name abc
```

poe pd-description

Syntax

poe pd-description *text*

undo poe pd-description

View

PoE interface view

Default level

2: System level

Parameters

text: Describes of the PD connected to a PoE interface, a string of 1 to 80 characters.

Description

Use **poe pd-description** to configure a description for the PD connected to a PoE interface.

Use **undo poe pd-description** to restore the default.

By default, no description is available for the PD connected to a PoE interface.

Examples

Configure the description for the PD connected to GigabitEthernet 1/0/1 as IP Phone for Room 101.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe pd-description IP Phone For Room 101
```

poe pd-policy priority

Syntax

poe pd-policy priority

undo poe pd-policy priority

View

System view

Default level

2: System level

Parameters

None

Description

Use **poe pd-policy priority** to enable the priority-based power management policy for PoE interfaces.

Use **undo poe pd-policy priority** to restore the default.

By default, the priority-based power management policy is disabled for PoE interfaces.

- If the policy is enabled, and the PoE interface needs to supply power to outside in the case that the PSE is overloaded, the system allows the PoE interface to enable the PoE function, but whether the power can be supplied depends on the PoE interface priority.
- If the policy is not enabled, and the PoE interface needs to supply power to outside in the case that the PSE is overloaded, the system will not allow the PoE interface to enable the PoE function.

Examples

Enable the priority-based power management policy for PoE interfaces.

```
<Sysname> system-view
[Sysname] poe pd-policy priority
```

poe priority

Syntax

```
poe priority { critical | high | low }  
undo poe priority
```

View

PoE interface view, PoE-profile view

Default level

2: System level

Parameters

critical: Sets the power priority of a PoE interface to **critical**. The PoE interface whose power priority level is **critical** operates in guaranteed mode. In other words, power is first supplied to the PD connected to this critical PoE interface.

high: Sets the power priority of a PoE interface to **high**.

low: Sets the power priority of a PoE interface to **low**.

Description

Use **poe priority** to configure a power priority level for a PoE interface.

Use **undo poe priority** to restore the default.

By default, the power priority of a PoE interface is **low**.

When the PoE power is insufficient, power is first supplied to PoE interfaces with a higher priority level.

If a PoE profile is already applied to a PoE interface, remove the application of the file to the PoE interface before configuring the interface in PoE-profile view.

If a PoE profile is applied to a PoE interface, remove the application of the file to the PoE interface before configuring the interface in PoE interface view.

If two PoE interfaces have the same priority level, the PoE interface with a smaller ID has the higher priority level.

Examples

Set the power priority of GigabitEthernet 1/0/1 to **critical**.

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] poe priority critical
```

Set the power priority of GigabitEthernet 1/0/1 to **critical** through a PoE profile.

```
<Sysname> system-view  
[Sysname] poe-profile abc  
[Sysname-poe-profile-abc-1] poe priority critical  
[Sysname-poe-profile-abc-1] quit  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] apply poe-profile name abc
```

poe update

Syntax

poe update { **full** | **refresh** } *filename* [**pse** *pse-id*]

View

System view

Default level

2: System level

Parameters

full: Specifies the upgrade of the PSE processing software in full mode when the software is unavailable.

refresh: Specifies the upgrade of the PSE processing software in refresh mode when the software is available.

filename: Specifies the name of the upgrade file, a string of 1 to 64 characters. This file must be in the root directory of the file system of the device.

pse *pse-id*: Specifies a PSE ID.

Description

Use **poe update** to upgrade the PSE processing software online.

If none of the PoE commands can be successfully executed, use the full mode to restore the PSE firmware. In any other case, use the full mode only when the refresh mode cannot work correctly.

If you do not provide the *pse-id* argument, the PSEs of all IRF member devices are upgraded.

Examples

```
# Upgrade the processing software of PSE 7 in service.  
<Sysname> system-view  
[Sysname] poe update refresh 0400_001.S19 pse 7
```

poe utilization-threshold

Syntax

poe utilization-threshold *utilization-threshold-value* **pse** *pse-id*

undo poe utilization-threshold **pse** *pse-id*

View

System view

Default level

2: System level

Parameters

utilization-threshold-value: Specifies the power alarm threshold in percentage, in the range of 1 to 99.

pse *pse-id*: Specifies a PSE ID.

Description

Use **poe utilization-threshold** to configure a power alarm threshold for the PSE.

Use **undo poe utilization-threshold** to restore the default power alarm threshold of the PSE.

By default, the power alarm threshold for the PSE is 80%.

The system sends a trap message when the power utilization exceeds the alarm threshold. If the power utilization always stays above the alarm threshold, the system does not send any trap message. Instead, when the percentage of the power utilization drops below the alarm threshold, the system sends a trap message again.

Examples

Set the power alarm threshold to 90% for PSE 7.

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

```
[Sysname] poe utilization-threshold 90 pse 7
```

poe-profile

Syntax

poe-profile *profile-name* [*index*]

undo poe-profile { **index** *index* | **name** *profile-name* }

View

System view

Default level

2: System level

Parameters

profile-name: Specifies the name of a PoE profile, a string of 1 to 15 characters. A PoE profile name begins with a letter (a through z or A through Z) and must not contain reserved keywords such as **undo**, **all**, **name**, **interface**, **user**, **poe**, **disable**, **max-power**, **mode**, **priority** and **enable**.

index: Specifies the index number of a PoE profile, in the range of 1 to 100.

Description

Use **poe-profile** *profile-name* to create a PoE profile and enter PoE-profile view.

Use **undo poe-profile** to delete the specified PoE profile.

If no index is specified, the system automatically assigns an index to the PoE profile, starting from 1.

If a PoE profile is already applied to a PoE interface, you cannot delete it. To delete the file, execute the **undo apply poe-profile** command to remove the application of the PoE profile to the PoE interface.

Examples

Create a PoE profile, name it **abc**, and specify the index number as **3**.

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

```
[Sysname] poe-profile abc 3
```

Cluster management configuration commands

Cluster management commands are supported only in non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

NDP configuration commands

display ndp

Syntax

display ndp [**interface** *interface-list*] [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format *interface-list* = { *interface-type* *interface-number* [**to** *interface-type* *interface-number*] } & <1-10>, where, *interface-type* is port type and *interface-number* is port number, and &<1-10> means that you can provide up to 10 port indexes/port index lists for this argument.

|: 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 ndp** to display NDP configuration information, which includes the interval to send NDP packets, the time for the receiving switch to hold NDP information and information about the neighbors of all ports.

Examples

Display NDP configuration information.

```
<Sysname> display ndp
```

```
Neighbor Discovery Protocol is enabled.
```

```
Neighbor Discovery Protocol Ver: 1, Hello Timer: 60(s), Aging Timer: 180(s)
```

```
Interface: GigabitEthernet1/0/1
```

```
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0
```

```
Interface: GigabitEthernet1/0/2
```

```

    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/3
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/4
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/5
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/6
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/7
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/8
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/9
    Status: Enabled, Pkts Snd: 768, Pkts Rvd: 766, Pkts Err: 0

    Neighbor 1:  Aging Time: 159(s)
    MAC Address  : 000f-e200-5111
    Host Name    : HP
    Port Name    : GigabitEthernet1/0/32
    Software Ver: V100R001B02D028SP01
    Device Name  : HP A5800-24G-PoE+ Switch
    Port Duplex  : AUTO
    Product Ver  : Alpha 1210
    BootROM Ver  : 212

Interface: GigabitEthernet1/0/10
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/11
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/12
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/13
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/14
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

```

Interface: GigabitEthernet1/0/15

Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

The rest is omitted.

Table 54 Command output

Field	Description
Neighbor Discovery Protocol is enabled	NDP is enabled globally on the current switch.
Neighbor Discovery Protocol Ver	Version of NDP.
Hello Timer	Interval to send NDP packets.
Aging Timer	Time for the receiving switch to hold NDP information.
Interface	Specified port.
Status	NDP state of a port.
Pkts Snd	Number of the NDP packets sent through the port.
Pkts Rvd	Number of the NDP packets received on the port.
Pkts Err	Number of the error NDP packets received on the port.
Neighbor 1: Aging Time	Aging time of NDP information for a neighbor switch.
MAC Address	MAC address of a neighbor switch.
Host Name	System name of a neighbor switch.
Port Name	Port name of a neighbor switch.
Software Ver	Software version of the neighbor switch.
Device Name	Switch model of a neighbor switch.
Port Duplex	Port duplex mode of a neighbor switch.
Product Ver	Product version of a neighbor switch.
BootROM Ver	Boot ROM version of a neighbor switch.

ndp enable

Syntax

In Layer 2 Ethernet port view or Layer 2 aggregate interface view:

ndp enable

undo ndp enable

In system view:

ndp enable [**interface** *interface-list*]

undo ndp enable [**interface** *interface-list*]

View

System view, Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument.

Description

Use **ndp enable** to enable NDP globally or for specified ports.

Use **undo ndp enable** to disable this feature globally or for specified ports.

By default, NDP is disabled globally and also on all ports.

Executed in system view, the **ndp enable** command enables NDP for the specified ports. Otherwise, the command enables NDP globally if you provide the **interface** *interface-list* parameter.

Executed in interface view, this command enables NDP only for the current port.

Configured in Layer 2 aggregate interface view, the configuration does not take effect on the member ports of the aggregation group that corresponds to the aggregate interface; configured on a member port of an aggregation group, the configuration takes effect only after the member port quit the aggregation group. For more information about link aggregation, see *Layer 2—LAN Switching Configuration Guide*.

Examples

Enable NDP globally.

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

Enable NDP for port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ndp enable
```

ndp timer aging

Syntax

ndp timer aging *aging-time*

undo ndp timer aging

View

System view

Default level

2: System level

Parameters

aging-time: Specifies the amount of time for a switch to keep the NDP packets it receives, in the range of 5 to 255 seconds.

Description

Use **ndp timer aging** to specify the amount of time that a switch should keep the NDP packets it received from the adjacent switch.

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

By default, a switch keeps incoming NDP packets for 180 seconds.

The lifetime of NDP packets cannot be shorter than the interval to send NDP packets; otherwise, the NDP table may become unstable.

Related commands: **ndp timer hello**.

Examples

```
# Set the lifetime of NDP packets to 100 seconds.
```

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

```
[Sysname] ndp timer aging 100
```

ndp timer hello

Syntax

ndp timer hello *hello-time*

undo ndp timer hello

View

System view

Default level

2: System level

Parameters

hello-time: Sets the interval to send NDP packets, in the range of 5 to 254 seconds.

Description

Use **ndp timer hello** to set the interval to send NDP packets.

Use **undo ndp timer hello** to restore the default.

By default, the interval to send NDP packets is 60 seconds.

The interval for sending NDP packets cannot be longer than the time for the receiving switch to hold NDP packets; otherwise, the NDP table may become unstable.

Related commands: **ndp timer aging**.

Examples

```
# Set the interval to send NDP packets to 80 seconds.
```

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

```
[Sysname] ndp timer hello 80
```

reset ndp statistics

Syntax

reset ndp statistics [**interface** *interface-list*]

View

User view

Default level

1: Monitor level

Parameters

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format *interface-list* = { *interface-type* *interface-number* [**to** *interface-type* *interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. If you provide this keyword, NDP statistics of the specified port will be cleared; otherwise, NDP statistics of all ports will be cleared.

Description

Use **reset ndp statistics** to clear NDP statistics.

Examples

```
# Clear NDP statistics of all ports.  
<Sysname> reset ndp statistics
```

NTDP configuration commands

display ntdp

Syntax

```
display ntdp [ | { 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 ntdp** to display NTDP configuration information.

Examples

```
# Display NTDP configuration information.  
<Sysname> display ntdp  
NTDP is running.
```

```
Hops      : 4
Timer     : 1 min
Hop Delay : 100 ms
Port Delay: 10 ms
Last collection total time: 92ms
```

Table 55 Command output

Field	Description
NTDP is running	NTDP is enabled globally on the local switch.
Hops	Hop count for topology collection.
Timer	Interval to collect topology information (after the cluster is created).
disable	Indicates that the switch is not a management switch and unable to perform periodical topology collection.
Hop Delay	Delay time for the switch to forward topology collection requests.
Port Delay	Delay time for a topology-collection request to be forwarded through a port.
Last collection total time	Time cost during the last topology collection.

display ntdp device-list

Syntax

```
display ntdp device-list [ verbose ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

verbose: Displays detailed switch information collected through NTDP.

|: 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 ntdp device-list** to display switch information collected through NTDP.

Information displayed may not be that of the latest switch if you do not execute the **ntdp explore** command before using this command.

Related commands: **ntdp explore**.

Examples

```
# Display switch information collected through NTDP.
```



```
<Sysname> display ntdp device-list
```

MAC	HOP	IP	Device
000f-e200-3900	2	192.168.0.138/24	HP A5800-24G-PoE+ Switch
000f-e200-5806	1	192.168.0.58/24	HP A5800-24G-PoE+ Switch
000f-e200-5104	0	192.168.0.51/24	HP A5120-24G EI Switch
000f-e200-5111	1	192.168.0.52/24	HP A5800AF-48G Switch
000f-e200-5600	2	192.168.0.56/24	HP A5800-24G Switch
000f-e200-0000	2	192.168.0.137/24	HP A5800-24G Switch
000f-e218-d0d0	2	192.168.0.65/24	HP A5800-24G Switch

Table 56 Command output

Field	Description
MAC	MAC address of a switch
HOP	Hops to the collecting switch
IP	IP address and mask length of the management VLAN interface on the switch
Device	Switch model

Display detailed switch information collected through NTDP.

```
<aaa 0.Sysname> display ntdp device-list verbose
```

```
Hostname   : aabbcc_1.Sysname
MAC        : 000f-e200-5806
Device     : HP A5800-24G-PoE+ Switch
IP         : 192.168.0.58/24
Version    :
  HP Comware Platform Software
  Comware Software Version 5.20 Alpha 1210
  Copyright (c) 2010-2011 Hewlett-Packard Development Company, L.P.
  HP A5800-24G-PoE+ Switch V100R001B02D028SP01
```

```
-----
Hop        : 3
Cluster    : Member device of cluster aabbcc , Administrator MAC: 000f-e227-afdb
Peer Hostname : aabbcc_10.HP
Peer MAC     : 000f-e200-5111
Peer Port ID : GigabitEthernet1/0/26
Native Port ID : GigabitEthernet1/0/11
Speed       : 100
Duplex      : FULL
```

Table 57 Command output

Field	Description
Hostname	System name of the switch.
MAC	MAC address of the switch.
Device	Switch model.

Field	Description
IP	IP address and subnet mask length of the management VLAN interface on the switch.
Version	Version information.
Hop	Hops from the current switch to the switch that collects topology information.
Cluster	<p>Role of the switch in the cluster:</p> <ul style="list-style-type: none"> • Member switch of cluster aaa—A member switch of the cluster aaa. • Administrator switch of cluster aaa—The management switch of the cluster aaa. • Candidate switch—A candidate switch of cluster aaa. • Independent switch—The switch is connected to the cluster, but it has not joined the cluster. This may be because the cluster function is not enabled on the switch.
Administrator MAC	MAC address of the management switch.
Peer Hostname	System name of a neighbor switch.
Peer MAC	MAC address of a neighbor switch.
Peer Port ID	Name of the peer port connected to the local port.
Native Port ID	Name of the local port to which a neighbor switch is connected.
Speed	Speed of the local port to which a neighbor switch is connected.
Duplex	Duplex mode of the local port to which a neighbor switch is connected.

display ntdp single-device

Syntax

```
display ntdp single-device mac-address mac-address [ | { begin | exclude | include }
regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

mac-address: Specifies the MAC address of the switch, in the format H-H-H.

|: 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 ntdp single-device mac-address** to display detailed NTDP information for a specified switch.

Examples

Display detailed NTPD information for the switch with a MAC address of 00E0-FC00-5111.

```
<Sysname> display ntdp single-device mac-address 00e0-fc00-5111
```

```
Hostname   : aabbcc_1.Sysname
MAC        : 000f-e200-5806
Device     : HP A5800-24G-PoE+ Switch
IP         : 192.168.0.58/24
Version    :
            HP Comware Platform Software
            Comware Software Version 5.20 Alpha 1210
            Copyright (c) 2010-2011 Hewlett-Packard Development Company, L.P.
            HP A5800-24G-PoE+ Switch V100R001B02D028SP01
```

```
-----
Hop        : 0
Cluster    : Administrator device of cluster test
Peer Hostname : test_10.Sysname
Peer MAC    : 000f-e200-5111
Peer Port ID : GigabitEthernet1/0/5
Native Port ID : GigabitEthernet1/0/22
Speed      : 1000
Duplex     : FULL
```

Table 58 Command output

Field	Description
Hostname	System name of the switch.
MAC	MAC address of the switch.
Device	Switch model.
IP	IP address and subnet mask length of the management VLAN interface on the switch.
Version	Version information.
Hop	Hops from the current switch to the switch that collects topology information.
Cluster	Role of the switch in the cluster: <ul style="list-style-type: none">• Member switch of cluster aaa—A member switch of the cluster aaa.• Administrator switch of cluster aaa—The management switch of the cluster aaa.• Candidate switch—A candidate switch of cluster aaa.• Independent switch—The switch is connected to the cluster, but it has not joined the cluster. This may be because the cluster function is not enabled on the switch.
Administrator MAC	MAC address of the management switch.
Peer Hostname	Host name of a neighbor switch.
Peer MAC	MAC address of a neighbor switch.
Peer Port ID	Name of the peer port connected to the local port.

Field	Description
Native Port ID	Name of the local port to which a neighbor switch is connected.
Speed	Speed of the local port to which a neighbor switch is connected.
Duplex	Duplex mode of the local port to which a neighbor switch is connected.

ntdp enable

Syntax

ntdp enable

undo ntdp enable

View

System view, Layer 2 Ethernet port view, Layer 2 aggregate interface view

Default level

2: System level

Parameters

None

Description

Use **ntdp enable** to enable NTDP globally or for specified ports.

Use **undo ntdp enable** to disable NTDP globally or for specified ports.

By default, NTDP is disabled globally and on all ports.

- Executed in system view, the command enables global NTDP. Executed in interface view, the command enables NTDP of the current port.
- Configured in Layer 2 aggregate interface view, the configuration does not take effect on the member ports of the aggregation group that corresponds to the aggregate interface. Configured on a member port of an aggregation group, the configuration takes effect only after the member port quit the aggregation group. For more information about link aggregation, see *Layer 2—LAN Switching Configuration Guide*.

Examples

Enable NTDP globally.

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

```
[Sysname] ntdp enable
```

Enable NTDP for port GigabitEthernet 1/0/1.

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

```
[Sysname] interface GigabitEthernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ntdp enable
```

ntdp explore

Syntax

ntdp explore

View

User view

Default level

2: System level

Parameters

None

Description

Use **ntdp explore** to start topology information collection manually.

Examples

```
# Start topology information collection manually.  
<Sysname> ntdp explore
```

ntdp hop

Syntax

```
ntdp hop hop-value  
undo ntdp hop
```

View

System view

Default level

2: System level

Parameters

hop-value: Specifies the maximum hop count for collecting topology information, in the range of 1 to 16.

Description

Use **ntdp hop** to set the maximum hop count for collecting topology information.

Use **undo ntdp hop** to restore the default.

By default, the maximum hop count is 3.

This command is only applicable to the topology-collecting switch. A bigger number of hops requires more memory of the topology-collecting switch.

Examples

```
# Set the hop count for topology information collection to 5.  
<Sysname> system-view  
[Sysname] ntdp hop 5
```

ntdp timer

Syntax

```
ntdp timer interval  
undo ntdp timer
```

View

System view

Default level

2: System level

Parameters

interval: Sets the interval (in minutes) to collect topology information, in the range of 0 to 65535. 0 means not to collect topology information.

Description

Use **ntdp timer** to configure the interval to collect topology information.

Use **undo ntdp timer** to restore the default.

By default, the interval to collect topology information is 1 minute.

The management switch can start to collect topology information only after the cluster is set up.

Examples

Set the interval to collect topology information to 30 minutes.

```
<Sysname> system-view  
[Sysname] ntdp timer 30
```

ntdp timer hop-delay

Syntax

ntdp timer hop-delay *delay-time*

undo ntdp timer hop-delay

View

System view

Default level

2: System level

Parameters

delay-time: Sets the delay time (in milliseconds) for a switch receiving topology-collection requests to forward them through its first port. The value range for this argument is 1 to 1000.

Description

Use **ntdp timer hop-delay** to set the delay time for the switch to forward topology-collection requests through the first port.

Use **undo ntdp timer hop-delay** to restore the default delay time.

By default, the delay time for the switch to forward topology-collection requests through the first port is 200 ms.

Examples

Set the delay time for the switch to forward topology-collection requests through the first port to 300 ms.

```
<Sysname> system-view  
[Sysname] ntdp timer hop-delay 300
```

ntdp timer port-delay

Syntax

ntdp timer port-delay *delay-time*

undo ntdp timer port-delay

View

System view

Default level

2: System level

Parameters

delay-time: Sets the delay time (in milliseconds) for a switch to forward a topology-collection request through its successive ports, in the range of 1 to 100.

Description

Use **ntdp timer port-delay** to set the delay time for a switch to forward a received topology-collection request through its successive ports.

Use **undo ntdp timer port-delay** to restore the default delay time.

By default, the delay time for a switch to forward a received topology-collection request through its successive ports is 20 ms.

Examples

Set the delay time for the switch to forward topology-collection requests through the successive ports to 40 ms.

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

```
[Sysname] ntdp timer port-delay 40
```

Cluster configuration commands

add-member

Syntax

add-member [*member-number*] **mac-address** *mac-address* [**password** *password*]

View

Cluster view

Default level

2: System level

Parameters

member-number: Specifies the member assigned to the candidate switch to be added to a cluster, in the range of 1 to 255.

mac-address: Specifies the MAC address of the candidate switch (in hexadecimal form of H-H-H).

password: Specifies the password of the candidate switch, a string of 1 to 16 characters. The password is required when you add a candidate switch to a cluster. However, this argument is not needed if the candidate switch is not configured with a super password.

Description

Use **add-member** to add a candidate switch to a cluster.

This command can be executed only on the management switch.

When you add a candidate switch to a cluster, if you do not assign a number to the switch, the management switch automatically assigns a usable number to the newly added member switch.

After a candidate switch joins the cluster, its level 3 password is replaced by the super password of the management switch in cipher text.

Examples

Add a candidate switch to the cluster on the management switch, setting the number to 6. (Assume that the MAC address and user password of the candidate switch are 00E0-FC00-35E7 and 123456 respectively.)

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] add-member 6 mac-address 00e0-fc00-35e7 password 123456
```

administrator-address

Syntax

administrator-address *mac-address* **name** *cluster-name*

undo administrator-address

View

Cluster view

Default level

2: System level

Parameters

mac-address: Specifies the MAC address of the management switch (in hexadecimal form of H-H-H).

cluster-name: Specifies the name of an existing cluster. It is a string of 1 to 8 characters, which can only be letters, numbers, hyphen (-), and underline (_).

Description

Use **administrator-address** to add a candidate switch to a cluster.

Use **undo administrator-address** to remove a member switch from the cluster.

By default, a switch belongs to no cluster.

The **administrator-address** command is applicable only on candidate switches, while the **undo administrator-address** command is applicable only on member switches.

To remove a cluster member from a cluster, use the **delete-member** command on the management switch.

Examples

Remove a member switch from the cluster on the member switch.

```
<aaa_1.Sysname> system-view
```



```
[aaa_1.Sysname] cluster
[aaa_1.Sysname-cluster] undo administrator-address
```

auto-build

Syntax

auto-build [**recover**]

View

Cluster view

Default level

2: System level

Parameters

recover: Automatically reestablishes communication with all the member switches.

Description

Use **auto-build** to establish a cluster automatically.

- This command can be executed on a candidate switch or the management switch.
- If you execute this command on a candidate switch, you will be required to enter the cluster name to build a cluster. Then the system will collect candidates and add the collected candidates into the cluster automatically.
- If you execute this command on the management switch, the system will collect candidates directly and add them into the cluster automatically.
- The **recover** keyword is used to recover a cluster. Using the **auto-build recover** command, you can find the members that are currently not in the member list and add them to the cluster again.
- Make sure NTDP is enabled, because it is the basis of candidate and member collection. The collection range is also decided through NTDP. You can use the **ntdp hop** command in system view to modify the collection range.
- If a member is configured with a super password different from the super password of the management switch, it cannot be automatically added to the cluster.

Examples

Establish a cluster automatically on the management switch.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] auto-build
Restore topology from local flash file,for there is no base topology.
(Please confirm in 30 seconds, default No). (Y/N)
n
Please input cluster name:test
Collecting candidate list, please wait...
#Jul 15 10:49:01:921 2009 Sysname CLST/4/RoleChange:
OID:1.3.6.1.4.1.25506.8.7.1.0.3: member 00.00.00.00.
00.22.57.ad.2c.f3 role change, NTDPIndex:0.00.00.00.00.00.22.57.ad.2c.f3, Role:1
Candidate list:
Name                               Hops  MAC Address      Device
HP                                1      000f-e200-a0b0   HP A5120-24G EI Switch
```

```

HP                3      000f-e2aa-0000  HP A5800-24G-PoE+ Switch
HP                3      000f-e200-7000  HP A5800-24G Switch
HP                2      000f-e200-0001  HP A5800-24G-PoE+ Switch

Processing...please wait
%Jul 15 10:49:03:451 2009 Sysname CLST/4/LOG:
Member 3030-3000-0001 is joined in cluster test.
%Jul 15 10:49:03:572 2009 Sysname CLST/4/LOG:
Member 00e0-faaa-0000 is joined in cluster test.
%Jul 15 10:49:03:692 2009 Sysname CLST/4/LOG:
Member 000f-e200-a0b0 is joined in cluster test.
%Jul 15 10:49:03:813 2009 Sysname CLST/4/LOG:
Member 000f-e200-7000 is joined in cluster test.

Cluster auto-build Finish!
4 member(s) added successfully.
[test_0.Sysname-cluster]

```

Table 59 Command output

Field	Description
Restore topology from local flash file,for there is no base topology. (Please confirm in 30 seconds, default No). (Y/N)	Whether to restore the topology information of the cluster from the Flash of the current switch. If there was once a cluster on your network and the standard topology information has been saved to the switch, you can select to restore the standard topology information. For more information about saving standard topology information, see the topology accept and topology save-to commands.

Establish a cluster automatically on the management switch and select to restore the standard topology from the local Flash.

```

<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] auto-build
Restore topology from local flash file,for there is no base topology.
(Please confirm in 30 seconds, default No). (Y/N)
y

Begin get base topology file from local flash.....
Get file OK
Begin build base topology from file.....
Finish building base topology from file
Begin build blacklist from file.....
Finish building blacklist from file

Please input cluster name:test
Collecting candidate list, please wait...

#Jul 15 10:54:30:069 2009 Sysname CLST/4/RoleChange:
OID:1.3.6.1.4.1.25506.8.7.1.0.3: member 00.00.00.00.

```

```
00.22.57.ad.2c.f3 role change, NTDPIndex:0.00.00.00.00.00.22.57.ad.2c.f3, Role:1
Candidate list:
```

Name	Hops	MAC Address	Device
HP	1	000f-e200-a0b0	HP A5120-24G EI Switch
HP	3	000f-e2aa-0000	HP A5800-24G-PoE+ Switch
HP	3	000f-e200-7000	HP A5800-24G Switch
HP	2	000f-e200-0001	HP A5800-24G-PoE+ Switch

```
Processing...please wait
%Jul 15 10:54:31:626 2009 Sysname CLST/4/LOG:
Member 000f-e200-a0b0 is joined in cluster test.
```

```
%Jul 15 10:54:31:747 2009 Sysname CLST/4/LOG:
Member 3030-3000-0001 is joined in cluster test.
```

```
%Jul 15 10:54:31:904 2009 Sysname CLST/4/LOG:
Member 000f-e200-7000 is joined in cluster test.
```

```
%Jul 15 10:54:32:035 2009 Sysname CLST/4/LOG:
Member 00e0-faaa-0000 is joined in cluster test.
```

```
Cluster auto-build Finish!
4 member(s) added successfully.
```

```
[test_0.Sysname-cluster]
```

Table 60 Command output

Field	Description
Begin get base topology file from local flash.....	Get the standard topology file from the local Flash, and the file name is topology.top .
Begin build base topology from file	Begin to restore topology from the standard topology file.
Begin build blacklist from file	Begin to get blacklist from the standard topology file.

black-list add-mac

Syntax

```
black-list add-mac mac-address
```

View

Cluster view

Default level

2: System level

Parameters

mac-address: Specifies the MAC address of the switch to be added into the blacklist, in the form of H-H-H.

Description

Use **black-list add-mac** to add a switch to the blacklist.

This command can be executed only on the management switch.

Examples

Add a switch with the MAC address of 0EC0-FC00-0001 to the blacklist on the management switch.

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] black-list add-mac 0ec0-fc00-0001
```

black-list delete-mac

Syntax

black-list delete-mac { **all** | *mac-address* }

View

Cluster view

Default level

2: System level

Parameters

all: Deletes all switches from the blacklist.

mac-address: Specifies the MAC address of the switch to be deleted from the blacklist, which is in the form of H-H-H.

Description

Use **black-list delete-mac** to delete a switch from the blacklist.

This command can be executed only on the management switch.

Examples

Delete a switch with the MAC address of 0EC0-FC00-0001 from the blacklist on the management switch.

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] black-list delete-mac 0ec0-fc00-0001
```

Delete all switches in the blacklist on the management switch.

```
[aaa_0.Sysname-cluster] black-list delete-mac all
```

build

Syntax

build *cluster-name*

undo build

View

Cluster view

Default level

2: System level

Parameters

cluster-name: Specifies the cluster name. It is a string of 1 to 8 characters, which can only be letters, numbers, hyphens (-), and underlines (_).

Description

Use **build** to configure the current switch as the management switch and specify a cluster name for it.

Use **undo build** to configure the current management switch as a candidate switch.

By default, the switch is not a management switch.

When executing this command, you will be asked whether to create a standard topology map or not.

This command can only be applied to switches that are capable of being a management switch and are not members of other clusters. The command takes no effect if you execute the command on a switch that is already a member of another cluster. If you execute this command on a management switch, you will replace the cluster name with the one you specify (suppose the new cluster name differs from the original one).

The number of the management switch in the cluster is 0.

Examples

Configure the current switch as a management switch and specify the cluster name as **aabbcc**.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 172.16.0.1 255.255.255.248
[Sysname-cluster] build aabbcc
Restore topology from local flash file,for there is no base topology.
(Please confirm in 30 seconds, default No). (Y/N)
n
#Apr 26 19:25:52:407 2000 Sysname CLST/4/RoleChange:
OID:1.3.6.1.4.1.25506.8.7.1.0.3: member 00.00.00.00.
e0.fc.00.58.06 role change, NTDPIndex:0.00.00.00.00.00.e0.fc.00.58.06, Role:1
%Apr 26 19:26:06:941 2000 Sysname CLST/4/LOG:
Member 000f-e200-0000 is joined in cluster aabbcc.
%Apr 26 19:26:07:041 2000 Sysname CLST/4/LOG:
Member 00e0-fc02-2180 is joined in cluster aabbcc.
%Apr 26 19:26:07:702 2000 Sysname CLST/4/LOG:
Member 000f-e218-d0d0 is joined in cluster aabbcc.
%Apr 26 19:26:08:014 2000 Sysname CLST/4/LOG:
Member 000f-cb00-5600 is joined in cluster aabbcc.
%Apr 26 19:26:08:546 2000 Sysname CLST/4/LOG:
Member 000f-e200-0144 is joined in cluster aabbcc.
```

Table 61 Command output

Field	Description
Restore topology from local flash file,for there is no base topology. (Please confirm in 30 seconds, default No). (Y/N)	Whether to restore the topology information of the cluster from the Flash of the current switch. If there was once a cluster on your network and the standard topology information has been saved to the switch, you can select to restore the standard topology information. For more information about saving the standard topology information, see the topology accept and topology save-to commands.
#Apr 26 19:25:52:407 2000 Sysname CLST/4/RoleChange: OID:1.3.6.1.4.1.25506.8.7.1.0.3: member 00.00.00.00.e0.fc.00.58.06 role change, NTDPIIndex:0.00.00.00.00.00.e0.fc.00.58.06, Role:1	Current switch becomes the management switch in the cluster.
%Apr 26 19:26:06:941 2000 Sysname CLST/4/LOG: Member 000f-e200-0000 is joined in cluster aabbcc.	Switch with a MAC address of 000f-e200-0000 has joined cluster aabbcc .

cluster

Syntax

cluster

View

System view

Default level

2: System level

Parameters

None

Description

Use **cluster** to enter cluster view.

Examples

```
# Enter cluster view
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster]
```

cluster enable

Syntax

cluster enable

undo cluster enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **cluster enable** to enable the cluster function.

Use **undo cluster enable** to disabled the cluster function.

By default, the cluster function is enabled.

- When you execute the **undo cluster enable** command on a management switch, you remove the cluster and its members, prevent the switch from functioning as a management switch, and disable the cluster function on the switch
- When you execute the **undo cluster enable** command on a member switch, you disable the cluster function on the switch, and the switch leaves the cluster.
- When you execute the **undo cluster enable** command on a switch that belongs to no cluster, you disable the cluster function on the switch.

Examples

```
# Enable the cluster function.  
<Sysname> system-view  
[Sysname] cluster enable
```

cluster switch-to

Syntax

```
cluster switch-to { member-number | mac-address mac-address | administrator | sysname  
member-sysname }
```

View

User view

Default level

0: Visit level

Parameters

member-number: Specifies the number of a member switch in a cluster, in the range of 1 to 255.

mac-address *mac-address*: Specifies the MAC address of a member switch, which is in the format H-H-H.

administrator: Switches from a member switch to the management switch.

sysname *member-sysname*: Specifies the system name of a member switch, a string of 1 to 32 characters.

Description

Use **cluster switch-to** to switch between the management switch and member switches.

Examples

Switch from the operation interface of the management switch to that of the member switch numbered 6 and then switch back to the operation interface of the management switch.

```
<aaa_0.Sysname> cluster switch-to 6
<aaa_6.Sysname> quit
<aaa_0.Sysname>
```

Enter the member switch numbered 2 with the system name of **5120-2**.

```
<aaa_0.Sysname> cluster switch-to sysname 5120-2
  SN   Device                               MAC Address   Status   Name
  2    HP A5120-24G EI Switch              000f-e2aa-0000 Up       aaa_2.5120-2
  3    HP A5120-24G EI Switch              000f-e200-0001 Up       aaa_3.5120-2
Please select a member-number to input: 2
Trying ...
Press CTRL+K to abort
Connected ...
*****
* Copyright (c) 2010-2011 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                *
* no decompiling or reverse-engineering shall be allowed.                    *
*****
<aaa_2.5800-2>
```

cluster-local-user

Syntax

cluster-local-user *user-name* [**password** { **cipher** | **simple** } *password*]
undo cluster-local-user *user-name*

View

Cluster view

Default level

1: Monitor level

Parameters

user-name: Specifies the username used for logging in to the switches within a cluster through Web, a string of 1 to 55 characters.

password: Specifies the password for logging in to the cluster member devices through Web. If this keyword is not specified, you can log in without a password.

cipher: Specifies a ciphertext password.

simple: Specifies a plaintext password.

auth-password: Specifies the password string. This argument is case sensitive. If **simple** is specified, it must be a string of 1 to 63 characters. If **cipher** is specified, it must be a ciphertext string of 1 to 117 characters.

Description

Use **cluster-local-user** to configure a Web user accounts in batches.

Use **undo cluster-local-user** to remove the configuration.

The command can be configured once only on the management switch.

Examples

On the management switch, configure a web user account for the cluster member switches.

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] cluster-local-user abc password simple 123456
```

cluster-mac

Syntax

cluster-mac *mac-address*

undo cluster-mac

View

Cluster view

Default level

2: System level

Parameters

mac-address: Specifies the multicast MAC address (in hexadecimal in the format H-H-H), which can be 0180-C200-0000, 0180-C200-000A, 0180-C200-0020 through 0180-C200-002F, or 010F-E200-0002.

Description

Use **cluster-mac** to configure the destination MAC address for cluster management protocol packets.

Use **undo cluster-mac** to restore the default.

By default, the destination MAC address for cluster management protocol packets is 0180-C200-000A.

This command can be executed only on the management switch.

Examples

Set the destination MAC address of the cluster management protocol packets to 0180-C200-0000 on the management switch.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] cluster-mac 0180-C200-0000
```

cluster-mac syn-interval

Syntax

cluster-mac syn-interval *interval*

View

Cluster view

Default level

2: System level

Parameters

interval: Sets the interval (in minutes) to send MAC address negotiation broadcast packets, in the range of 0 to 30. If the interval is set to 0, the management switch does not send broadcast packets to the member switches.

Description

Use **cluster-mac syn-interval** to set the interval for a management switch to send MAC address negotiation broadcast packets for cluster management.

By default, the interval is set to one minute.

This command can be executed only on the management switch.

Examples

Set the interval for the management switch to send MAC address negotiation broadcast packets for cluster management to two minutes on the management switch.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] cluster-mac syn-interval 2
```

cluster-snmp-agent community

Syntax

cluster-snmp-agent community { read | write } community-name [mib-view view-name]

undo cluster-snmp-agent community community-name

View

Cluster view

Default level

1: Monitor level

Parameters

read: Indicates to allow the community's read-only access to MIB objects. The community with read-only authority can only query the switch information.

write: Indicates to allow the community's read-write access to MIB objects. The community with read-write authority can configure the switch information.

community-name: Specifies the community name, a string of 1 to 26 characters.

view-name: Specifies the MIB view name, a string of 1 to 32 characters.

Description

Use **cluster-snmp-agent community** to configure an SNMP community shared by a cluster and set its access authority.

Use **undo cluster-snmp-agent community** to remove a specified community name.

The command used to configure the SNMP community with read-only or read-and-write authority can only be executed once on the management switch. This configuration will be synchronized to the member switches on the whitelist, which is equivalent to configuring multiple member switches at one time.

An SNMP community name is retained when a cluster is dismissed or a member switch is removed from the whitelist.

If the same community name as the current one has been configured on a member switch, the current community name will replace the original one.

Examples

Configure the SNMP community name shared by a cluster as **comaccess** and allow the community's read-only access to MIB objects.

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] cluster-snmp-agent community read comaccess
```

Configure the SNMP community name shared by a cluster as **comaccesswr** and allow the community's read-write access to MIB objects.

```
[aaa_0.Sysname-cluster] cluster-snmp-agent community write comaccesswr
```

cluster-snmp-agent group v3

Syntax

```
cluster-snmp-agent group v3 group-name [ authentication | privacy ] [ read-view read-view ]
[ write-view write-view ] [ notify-view notify-view ]
```

```
undo cluster-snmp-agent group v3 group-name [ authentication | privacy ]
```

View

Cluster view

Default level

1: Monitor level

Parameters

group-name: Specifies the group name, a string of 1 to 32 characters.

authentication: Specifies to authenticate a packet but not to encrypt it.

privacy: Specifies to authenticate and encrypt a packet.

read-view: Specifies the read-only view name, a string of 1 to 32 characters.

write-view: Specifies the read-write view name, a string of 1 to 32 characters.

notify-view: Specifies the view name in which trap messages can be sent. It is a string of 1 to 32 characters.

Description

Use **cluster-snmp-agent group** to configure the SNMPv3 group shared by a cluster and set its access rights.

Use **undo cluster-snmp-agent group** to remove the SNMPv3 group shared by a cluster.

The command can be executed once only on the management switch. This configuration will be synchronized to the member switches on the whitelist, which is equivalent to configuring multiple member switches at one time.

The SNMPv3 group name is retained when a cluster is dismissed or a member switch is deleted from the whitelist.

If the same group name as the current one has been configured on a member switch, the current group name will replace the original one.

Examples

```
# Create an SNMP group snmpgroup.
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] cluster-snmp-agent group v3 snmpgroup
```

cluster-snmp-agent mib-view

Syntax

cluster-snmp-agent mib-view included *view-name oid-tree*
undo cluster-snmp-agent mib-view *view-name*

View

Cluster view

Default level

1: Monitor level

Parameters

included: Includes MIB views.

view-name: Specifies the MIB view name, a string of 1 to 32 characters.

oid-tree: Specifies the MIB subtree. It is a string of 1 to 255 characters, which can only be a variable OID string or variable name string. OID is composed of a series of integers, indicating where a node is in the MIB tree. It can uniquely identify an object in a MIB.

Description

Use **cluster-snmp-agent mib-view** to create or update MIB view information shared by a cluster.

Use **undo cluster-snmp-agent mib-view** to delete MIB view information shared by a cluster.

By default, the MIB view name shared by a cluster is ViewDefault, in which the cluster can access an ISO subtree.

This command can be executed once only on the management switch. This configuration will be synchronized to member switches on the whitelist, which is equivalent to configuring multiple member switches at one time.

The MIB view is retained when a cluster is dismissed or a member switch is deleted from the whitelist.

If the same view name as the current one has been configured on a member switch, the current view will replace the original one on the member switch.

Examples

```
# Create a view including all objects of mib2.
```

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] cluster-snmp-agent mib-view included mib2 1.3.6.1.2.1
```

cluster-snmp-agent usm-user v3

Syntax

cluster-snmp-agent usm-user v3 *user-name group-name* [**authentication-mode** { **md5** | **sha** } [**cipher** | **simple**] *auth-password* [**privacy-mode** **des56** [**cipher** | **simple**] *priv-password*]]

undo cluster-snmp-agent usm-user v3 *user-name group-name*

View

Cluster view

Default level

1: Monitor level

Parameters

user-name: Specifies a username, a string of 1 to 32 characters.

group-name: Specifies an SNMP group name, a string of 1 to 32 characters.

authentication-mode: Enables authentication for the SNMP user.

md5: Specifies HMAC-MD5-96 as the authentication algorithm.

sha: Specifies HMAC-SHA-96 as the authentication algorithm.

cipher: Specifies a ciphertext authentication key.

simple: Specifies a plaintext authentication key.

auth-password: Specifies the authentication 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 string.

privacy-mode: Enables encryption.

des56: Specifies DES as the encryption protocol.

priv-password: Specifies the privacy 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 string.

Description

Use **cluster-snmp-agent usm-user v3** to add a new user to the SNMPv3 group shared by a cluster.

Use **undo cluster-snmp-agent usm-user v3** to delete the SNMPv3 group user shared by the cluster.

The command can be executed once on the management switch only. This configuration will be synchronized to member switches on the whitelist, which is equal to configuring multiple member switches at one time.

The SNMPv3 group user is retained when a cluster is dismissed or a member switch is deleted from the whitelist.

If the same username as the current one has been configured on a member switch, the current username will replace the original one on the member switch.

Examples

Add a user **wang** to the SNMP group **snmpgroup**, set the security level to authentication-needed and specify the authentication protocol as HMAC-MD5-96, and specify the authentication password as **pass**.

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] cluster-snmp-agent usm-user v3 wang snmpgroup
authentication-mode md5 pass
```

delete-member

Syntax

delete-member *member-number* [**to-black-list**]

View

Cluster view

Default level

2: System level

Parameters

member-number: Specifies the number of a member switch in a cluster, in the range of 1 to 255.

to-black-list: Adds the switch removed from a cluster to the blacklist to prevent it from being added to the cluster again.

Description

Use **delete-member** to remove a member switch from the cluster.

This command can be executed only on the management switch.

If you only remove a member switch from the cluster without adding it to the blacklist, the switch will be automatically added to the cluster again.

Examples

On the management switch, remove the member switch numbered 2 from the cluster and add it to the blacklist.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] delete-member 2 to-black-list
```

display cluster

Syntax

display cluster [| { **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 cluster** to display information about the cluster to which the current switch belongs.

This command can be executed only on the management switch and member switches.

Examples

Display information about the cluster to which the current switch belongs on the management switch.

```
<aaa_0.Sysname> display cluster
Cluster name:"aaa"
Role:Administrator
Management-vlan:100
Handshake timer:10 sec
Handshake hold-time:60 sec
IP-Pool:1.1.1.1/16
cluster-mac:0180-c200-000a
No logging host configured
No SNMP host configured
No FTP server configured
No TFTP server configured
```

2 member(s) in the cluster, and 0 of them down.

Display information about the cluster to which the current switch belongs on a member switch.

```
<aaa_1.Sysname> display cluster
Cluster name:"aaa"
Role:Member
Member number:1
Management-vlan:100
cluster-mac:0180-c200-000a
Handshake timer:10 sec
Handshake hold-time:60 sec

Administrator device IP address:1.1.1.1
Administrator device mac address:00e0-fc00-1d00
Administrator status:Up
```

Table 62 Command output

Field	Description
Cluster name	Name of the cluster.

Field	Description
Role	Role of the switch in the cluster: <ul style="list-style-type: none"> • Administrator—The current switch is a management switch. • Member—The current switch is a member switch.
Member number	Number of the switch in the cluster.
Management-vlan	Management VLAN of the cluster.
Handshake timer	Interval to send handshake packets.
Handshake hold-time	Value of handshake timer.
IP-Pool	Private IP addresses of the member switches in the cluster.
cluster-mac	Multicast MAC address of cluster management packets.
Administrator device IP address	IP address of the management switch.
Administrator device mac address	MAC address of the management switch.
Administrator status	State of the management switch.

display cluster base-topology

Syntax

```
display cluster base-topology [ mac-address mac-address | member-id member-number ] [ | { begin | exclude | include } regular-expression ]
```

View

Any view

Default level

2: System level

Parameters

mac-address: Specifies a switch by its MAC address. The system displays the standard topology with the switch as the root.

member-number: Specifies a switch by its number. The system displays the standard topology with the switch as the root.

|: 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 cluster topology** to display standard topology information for a cluster.

You can create a standard topology map when executing the **build** or **auto-build** command, or you can use **topology accept** to save the current topology map as the standard topology map.

This command can be executed only on the management switch.

Examples

Display the standard topology of a cluster.

```
<aaa_0.Sysname> display cluster base-topology
-----
      (PeerPort) ConnectFlag (NativePort) [SysName:DeviceMac]
-----
[aaa_0.Sysname:0022-57ad-2cf3]
|
L- (P_2)<-->(P_2) [aaa_1.5820:000f-e200-a0b0]
|
|  |-- (P_2/0/25)<-->(P_3/0/1) [aaa_4.5800-2:3030-3000-0001]
|  |  |
|  |  |-- (P_3/0/5)<-->(P_1/0/1) [aaa_3.55EI-2:000f-e200-7000]
|  |  |
|  |  L- (P_3/0/3)<-->(P_5/0/3) [aaa_2.5800-3:00e0-faaa-0000]
|  |  |
|  L- (P_3/0/15)<-->(P_5/0/1) [aaa_2.5800-3:00e0-faaa-0000]
```

Table 63 Command output

Field	Description
PeerPort	Peer port
ConnectFlag	Connection flag: <-->
NativePort	Local port
SysName	System name of the peer switch
DeviceMac	MAC address of the peer switch

display cluster black-list

Syntax

display cluster black-list [| { **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 *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 cluster black-list** to display the current blacklist of a cluster.

This command can be executed only on the management switch.

Examples

Display the current blacklist of the cluster.

```
<aaa_0.Sysname> display cluster black-list
Device ID           Access Device ID       Access port
00e0-fc00-0010      00e0-fc00-3550         GigabitEthernet1/0/1
```

Table 64 Command output

Field	Description
Device ID	ID of the blacklist switch, indicated by its MAC address.
Access Device ID	ID of the switch connected to the blacklist switch, indicated by its MAC address.
Access port	Port connected to the blacklist switch.

display cluster candidates

Syntax

display cluster candidates [**mac-address** *mac-address* | **verbose**] [[{ **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

mac-address *mac-address*: Specifies the MAC address of a candidate switch, which is in the format H-H-H.

verbose: Displays the detailed information about a candidate switch.

[: 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 cluster candidates** to display information about the candidate switches of a cluster.

The command can be executed only on the management switch.

Examples

Display information about all candidate switches.

```

<aaa_0.Sysname> display cluster candidates
  MAC           HOP  IP           Device
  000f-e200-0001  2           HP A5800-24G-PoE+ Switch
  000f-e2aa-0000  3           HP A5800-24G-PoE+ Switch

# Display information about a specified candidate switch.

<aaa_0.Sysname> display cluster candidates mac-address 3030-3000-0001
  Hostname   : 5800-2
  MAC        : 000f-e200-0001
  Hop        : 2
  Device     : HP A5800-24G-PoE+ Switch
  IP         :

# Display detailed information about all candidate switches.

<aaa_0.Sysname> display cluster candidates verbose
  Hostname   : 5800-2
  MAC        : 000f-e200-0001
  Hop        : 2
  Device     : HP A5800-24G-PoE+ Switch
  IP         :

  Hostname   : 5800-3
  MAC        : 000f-e2aa-0000
  Hop        : 3
  Device     : HP A5800-24G-PoE+ Switch
  IP         :

```

Table 65 Command output

Field	Description
Hostname	System name of a candidate switch
MAC	MAC address of a candidate switch
Hop	Hops from a candidate switch to the management switch
IP	IP address of a candidate switch
Device	Model of a candidate switch

display cluster current-topology

Syntax

```

display cluster current-topology [ mac-address mac-address [ to-mac-address mac-address ] |
member-id member-number [ to-member-id member-number ] ] [ | { begin | exclude | include }
regular-expression ]

```

View

Any view

Default level

2: System level

Parameters

member-number: Specifies the number of the switches in a cluster (including the management switch and member switches).

mac-address: Specifies the MAC addresses of the switches in a cluster (including the management switch and member 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 cluster current-topology** to display information about the current topology of a cluster.

- If you specify both the **mac-address** *mac-address* and **to-mac-address** *mac-address* arguments, the topology information of the switches that are in a cluster and form the connection between two specified switches is displayed.
- If you specify both the **member-id** *member-number* and **to-member-id** *member-number* arguments, the topology information of the switches that are in a cluster and form the connection between two specified switches is displayed.
- If you specify only the **mac-address** *mac-address* or **member-id** *member-number* argument, the topology information of all the switches in a cluster is displayed, with a specified switch as the root node.

This command can be executed only on the management switch.

Examples

Display information about the current topology of a cluster.

```
<aaa_0.Sysname> display cluster current-topology

-----
      (PeerPort) ConnectFlag (NativePort) [SysName:DeviceMac]
-----

ConnectFlag:
  <--> normal connect    --> odd connect    **** in blacklist
  ???? lost device      ++++ new device    -| |- STP,RRPP discarding
-----

[aaa_0.Sysname:0022-57ad-2cf3]
|
  L- (P_2)<-->(P_2) [aaa_1.5820:000f-e200-a0b0]
  |
    |-(P_2/0/25)<-->(P_3/0/1) [aaa_3.5800-2:3030-3000-0001]
    | |
    | |-(P_3/0/3)<-->(P_5/0/3) [aaa_2.5800-3:00e0-faaa-0000]
    | |
    | | L- (P_3/0/5) **** (P_1/0/1) [55EI-2:000f-e200-7000]
    |
    L- (P_3/0/15) -| |- (P_5/0/1) [aaa_2.5800-3:00e0-faaa-0000]
```

Table 66 Command output

Field	Description
PeerPort	Peer port.
ConnectFlag	Connection flag.
NativePort	Local port.
SysName:DeviceMac	System name of the switch.
<--> normal connect	Indicates a normal connection between the switch and the management switch.
--> odd connect	Indicates a unidirectional connection between the switch and the management switch.
**** in blacklist	Indicates the switch is in the blacklist.
???? lost device	Indicates a lost connection between the switch and the management switch.
++++ new device	Indicates that this is a new switch, whose identity is to be recognized by the administrator.
- - STP discarding	STP is blocked.

A new switch in the topology information is identified based on the standard topology. After you add a switch into a cluster, if you do not use the **topology accept** command to confirm the current topology and save it as the standard topology, this switch is still regarded as a new switch.

display cluster members

Syntax

```
display cluster members [ member-number | verbose ] [ | { begin | exclude | include }
regular-expression ]
```

View

Any view

Default level

1: Monitor level

Parameters

member-number: Specifies the number of the member switch, in the range of 0 to 255.

verbose: Displays the detailed information about all the switches in a cluster.

|: 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 cluster members** to display the information about cluster members.

This command can be executed only on the management switch.

Examples

Display information about all switches in a cluster.

```
<aaa_0.Sysname> display cluster members
```

SN	Device	MAC Address	Status	Name
0	HP A5120-48G-PoE+ EI Switch w~	000f-e2ad-2cf3	Admin	aaa_0.Sysname
1	HP A5800-24G Switch	000f-e200-a0b0	Up	aaa_1.A5800
2	HP A5800-24G Switch	000f-e2aa-0000	Up	aaa_2.A5800-3
3	HP A5800-24G Switch	000f-e200-0001	Up	aaa_3.A5800-2

Table 67 Command output

Field	Description
SN	Number of the cluster member.
Device	Switch model.
MAC Address	MAC address of a switch.
Status	State of a switch: <ul style="list-style-type: none">• up—The member switch that is up.• down—The member that is down.• deleting— The member that is being deleted.• admin—The management switch.
Name	System name of a switch.

Display detailed information for the management switch and all member switches.

```
<aaa_0.Sysname> display cluster members verbose
```

Member number:0

Name:aaa_0.Sysname

Device: HP A5120-48G-PoE+ EI Switch with 2 Interface Slots

MAC Address: 000f-e2ad-2cf3

Member status:Admin

Hops to administrator device:0

IP: 121.1.1.4/16

Version:

HP Comware Platform Software

Comware Software Version 5.20 Release 2208

Copyright (c) 2010-2011 Hewlett-Packard Development Company, L.P.

HP A5120-48G-PoE+ EI Switch with 2 Interface Slots V300R001B05D025

Member number:1

Name:aaa_1.A5800

Device: HP A5800-24G Switch

MAC Address:000f-e200-a0b0

Member status:Up

```

Hops to administrator device:1
IP: 121.1.1.2/16
Version:
  HP Comware Platform Software
  Comware Software Version 5.20 Release 1211
  Copyright (c) 2010-2011 Hewlett-Packard Development Company, L.P.
  HP A5800-24G Switch V100R001B02D030

```

```

Member number:2
Name:aaa_2.A5800-3
Device: HP A5800-24G Switch
MAC Address:000f-e2aa-0000
Member status:Up
Hops to administrator device:3
IP:
Version:
  HP Comware Platform Software
  Comware Software Version 5.20 Release 1211
  Copyright (c) 2010-2011 Hewlett-Packard Development Company, L.P.
  HP A5800-24G Switch V100R001B02D030

```

```

Member number:3
Name:aaa_3.A5800-2
Device: HP A5800-24G Switch
MAC Address:000f-e200-0001
Member status:Up
Hops to administrator device:2
IP:
Version:
  HP Comware Platform Software
  Comware Software Version 5.20 Release 1211
  Copyright (c) 2010-2011 Hewlett-Packard Development Company, L.P.
  HP A5800-24G Switch V100R001B02D030

```

Table 68 Command output

Field	Description
Member number	Number of the cluster member.
Name	Name of a member switch, composed of the cluster name and the system name of the member switch, in the format cluster name.systemname. When the management switch type is not consistent with the member switch type, if a user modifies the cluster name on the management switch continuously, the cluster name may appear twice in the cluster member name, for example, "clustername.clustername.systemname". This abnormal case can restore in a period of time.
Device	Switch model.
MAC Address	MAC address of a switch.

Field	Description
Member status	State of a switch.
Hops to administrator device	Hops from the current member switch to the management switch.
IP	IP address of a member switch.
Version	Software version of the current member switch.

ftp-server

Syntax

```
ftp-server ip-address [ user-name username password { simple | cipher } password ]
undo ftp-server
```

View

Cluster view

Default level

3: Manage level

Parameters

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

username: Specifies the username used to log in to the FTP server, a string of 1 to 32 characters.

cipher: Specifies a ciphertext password.

simple: Specifies a plaintext password.

auth-password: Specifies the password 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 string.

Description

Use **ftp-server** to configure a public FTP server (by setting its IP address, username, and password) on the management switch for the member switches in the cluster.

Use **undo ftp-server** to remove the FTP server configured for the member switches in the cluster.

By default, a cluster is not configured with a public FTP server.

The command can be executed only on the management switch.

Examples

Set the IP address, username and password of an FTP server shared by the cluster on the management switch to be **1.0.0.9**, **ftp**, and **ftp** respectively.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] ftp-server 1.0.0.9 user-name ftp password simple ftp
```


holdtime

Syntax

holdtime *hold-time*

undo holdtime

View

Cluster view

Default level

2: System level

Parameters

hold-time: Sets the holdtime in the range of 1 to 255 seconds.

Description

Use **holdtime** to configure the holdtime of a switch.

Use **undo holdtime** to restore the default.

By default, the holdtime of a switch is 60 seconds.

This command can be executed only on the management switch.

The configuration is valid on all member switches in a cluster.

Examples

Set the holdtime to 30 seconds on the management switch.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] holdtime 30
```

ip-pool

Syntax

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

undo ip-pool

View

Cluster view

Default level

2: System level

Parameters

ip-address: Specifies the private IP address of the management switch in a cluster.

{ *mask* | *mask-length* }: Specifies the mask of the IP address pool of a cluster. It is an integer or in dotted decimal notation. When it is an integer, its value range is 1 to 30. A network address can be obtained by ANDing this mask with the private IP address of the administrator switch. The private IP addresses of all member switches in a cluster belong to this network segment.

Description

Use **ip-pool** to configure a private IP address range for cluster members.

Use **undo ip-pool** to remove the IP address range configuration.

By default, no private IP address range is configured for cluster members.

You must configure the IP address range only on the management switch and before establishing a cluster. If a cluster has already been established, you are not allowed to change the IP address range.

For a cluster to work normally, the IP addresses of the VLAN interfaces of the management switch and member switches must not be in the same network segment as that of the cluster address pool.

Examples

```
# Configure the IP address range of a cluster.
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.200.0.1 20
```

logging-host

Syntax

logging-host *ip-address*
undo logging-host

View

Cluster view

Default level

2: System level

Parameters

ip-address: Specifies the IP address of the logging host.

Description

Use **logging-host** to configure a logging host shared by a cluster.

Use **undo logging-host** to remove the logging host configuration.

By default, no logging host is configured for a cluster.

This command can be executed only on the management switch.

You have to execute the **info-center loghost** command in system view first for the logging host you configured to take effect.

For more information about the **info-center loghost** command, see "[Information center configuration commands](#)."

Examples

```
# Configure the IP address of the logging host shared by a cluster on the management switch as 10.10.10.9.
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
```

```
[aaa_0.Sysname-cluster] logging-host 10.10.10.9
```

management-vlan

Syntax

management-vlan *vlan-id*

undo management-vlan

View

System view

Default level

2: System level

Parameters

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

Description

Use **management-vlan** to specify the management VLAN.

Use **undo management-vlan** to restore the default.

By default, VLAN 1 is the management VLAN.

The management VLAN must be specified before a cluster is created. Once a member switch is added to a cluster, the management VLAN configuration cannot be modified. To modify the management VLAN for a switch belonging to a cluster, you need to cancel the cluster-related configurations on the switch, specify the desired VLAN to be the management VLAN, and then re-create the cluster.

For the purpose of security, you are not recommended to configure the management VLAN as the default VLAN ID of the port connecting the management switch and the member switches.

Only when the default VLAN ID of all cascade ports and the port connecting the management switch and the member switch is the management VLAN, can the packets in the management VLAN packets be passed without a tag. Otherwise, you must configure the packets from a management VLAN to pass these ports. For the more information about the configuration procedure, see *Layer 2—LAN Switching Configuration Guide*.

Examples

Specify VLAN 2 as the management VLAN.

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

```
[Sysname] management-vlan 2
```

management-vlan synchronization enable

Syntax

management-vlan synchronization enable

undo management-vlan synchronization enable

View

Cluster view

Default level

1: Monitor level

Parameters

None

Description

Use **management-vlan synchronization enable** to enable the management VLAN autonegotiation function.

Use **undo management-vlan synchronization enable** to disable the management VLAN autonegotiation function.

By default, the management VLAN autonegotiation function is disabled.

Examples

Enable the management VLAN autonegotiation function on the management switch.

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] management-vlan synchronization enable
```

nm-interface vlan-interface

Syntax

nm-interface vlan-interface *interface-name*

View

Cluster view

Default level

2: System level

Parameters

interface-name: Specifies the ID of the VLAN interface. The value range is the same as that of the existing VLAN interface ID.

Description

Use **nm-interface vlan-interface** to configure the VLAN interface of the access management switch (including FTP/TFTP server, management host and log host) as the network management interface of the management switch.

Examples

Configure VLAN-interface 2 as the network management interface.

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] nm-interface vlan-interface 2
```

reboot member

Syntax

reboot member { *member-number* | **mac-address** *mac-address* } [**eraseflash**]

View

Cluster view

Default level

2: System level

Parameters

member-number: Specifies the number of the member switch, in the range of 1 to 255.

mac-address *mac-address*: Specifies the MAC address of the member switch to be rebooted, in the format H-H-H.

eraseflash: Deletes the configuration file when a member switch reboots.

Description

Use **reboot member** to reboot a specified member switch.

This command can be executed only on the management switch.

Examples

Reboot the member switch numbered 2 on the management switch.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] reboot member 2
```

snmp-host

Syntax

snmp-host *ip-address* [**community-string read** *string1* **write** *string2*]

undo snmp-host

View

Cluster view

Default level

3: Manage level

Parameters

ip-address: Specifies the IP address of an SNMP host.

string1: Specifies the community name of read-only access, a string of 1 to 26 characters.

string2: Specifies the community name of read-write access, a string of 1 to 26 characters.

Description

Use **snmp-host** to configure a shared SNMP host for a cluster.

Use **undo snmp-host** to cancel the SNMP host configuration.

By default, no SNMP host is configured for a cluster.

This command can be executed only on the management switch.

Examples

```
# Configure a shared SNMP host for the cluster on the management switch.
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] snmp-host 1.0.0.9 community-string read 123 write 456
```

tftp-server

Syntax

tftp-server *ip-address*

undo tftp-server

View

Cluster view

Default level

2: System level

Parameters

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

Description

Use **tftp-server** to configure a shared TFTP server for a cluster.

Use **undo tftp-server** to cancel the TFTP server of the cluster.

By default, no TFTP server is configured.

This command can be executed only on the management switch.

Examples

```
# Configure a shared TFTP server on the management switch as 1.0.0.9.
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] tftp-server 1.0.0.9
```

timer

Syntax

timer *interval*

undo timer

View

Cluster view

Default level

2: System level

Parameters

interval: Specifies the interval (in seconds) to send handshake packets. The value range for this argument is 1 to 255.

Description

Use **timer** to set the interval to send handshake packets.

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

By default, the interval to send handshake packets is 10 seconds.

This command can be executed only on the management switch.

This configuration is valid for all member switches in a cluster.

Examples

Configure the interval to send handshake packets as 3 seconds on the management switch.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] timer 3
```

topology accept

Syntax

topology accept { **all** [**save-to** { **ftp-server** | **local-flash** }] | **mac-address** *mac-address* | **member-id** *member-number* }

undo topology accept { **all** | **mac-address** *mac-address* | **member-id** *member-number* }

View

Cluster view

Default level

2: System level

Parameters

all: Accepts the current cluster topology information as the standard topology information.

mac-address *mac-address*: Specifies a switch by its MAC address. The switch will be accepted to join the standard topology of the cluster.

member-id *member-number*: Specifies a switch by its number. The switch will be accepted to join the standard topology of the cluster. The *member-number* argument represents the number of a cluster member in the range of 0 to 255.

save-to: Confirms the current topology as the standard topology, and backs up the standard topology on the FTP server or local flash in a file named "topology.top".

Description

Use **topology accept** to confirm the current topology and save it as the standard topology.

Use **undo topology accept** to delete the standard topology.

This command can be executed only on the management switch.

The file used to save standard topology on the FTP server or the local Flash is named "topology.top", which includes the information of both blacklist and the whitelist. A blacklist contains the devices that are prohibited from being added to a cluster. A whitelist contains devices that can be added to a cluster.

Examples

```
# Take the current topology as the standard topology on the management switch.
```

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] topology accept all
```

topology restore-from

Syntax

```
topology restore-from { ftp-server | local-flash }
```

View

Cluster view

Default level

2: System level

Parameters

ftp-server: Restores the standard topology from the FTP server.

local-flash: Restores the standard topology from the local flash.

Description

Use **topology restore-from** to restore the standard topology in case the cluster topology is incorrect.

This command can be executed only on the management switch.

If the stored standard topology is not correct, the switch cannot be aware of it. Therefore, you must make sure the standard topology is correct.

Examples

```
# Restore the standard topology on the management switch.
```

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] topology restore-from local-flash
```

topology save-to

Syntax

```
topology save-to { ftp-server | local-flash }
```

View

Cluster view

Default level

2: System level

Parameters

ftp-server: Saves the standard topology to the FTP server.

local-flash: Saves the standard topology to the local flash.

Description

Use **topology save-to** to save the standard topology to the FTP server or the local flash.

The file used to save the standard topology on the FTP server or the local Flash is named "topology.top", which includes the information of both the blacklist and the whitelist. A blacklist contains the devices that are prohibited from being added to a cluster. A whitelist contains devices that can be added to a cluster.

This command can be executed only on the management switch.

Examples

Save the standard topology to the local flash on the management switch.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] topology save-to local-flash
```

Stack management configuration commands

display stack

Syntax

display stack [**members**] [[{ **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

members: Displays stack information for the stack members, including the master device and the member devices. This keyword is only available on the stack master.

[: 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 stack** to display stack information.

Examples

Display stack information on the master device.

```
<stack_0.Sysname> display stack
```

```
Role: Master
```

```
Management VLAN: 1
```

```
IP pool: 1.1.1.1/24
```

```
Device total number: 3
```

Display stack information on a member device.

```
<stack_1.Sysname> display stack
```

```
Role: Slave
```

```
Management VLAN: 1
```

```
IP pool: 1.1.1.1/24
```

```
Master MAC address: 000f-e200-1000
```

Table 69 Command output

Field	Description
Role	Role of the device in the stack: <ul style="list-style-type: none"> • Master—The device is the master device. • Slave—The device is a member device.
Management VLAN	VLAN for transmitting stack control packets between the stack master device and the member devices.
IP pool	Range of private IP addresses used by the stack.
Device total number	Total number of devices in the stack. This field is available only on the master device.
Master MAC address	MAC address of the master device. This field is available only on stack member devices.

Display stack information for all stack members on the master.

```
<stack_0.Sysname> display stack members
```

```
Number: 0
```

```
Role: Master
```

```
Sysname: stack_0.Sysname
```

```
Device type: HP A5120-48G-PoE+ EI Switch with 2 Interface Slots
```

```
MAC Address: 000f-e200-1000
```

```
Number: 1
```

```
Role: Slave
```

```
Sysname: stack_1.Sysname
```

```
Device type: HP A5120-48G-PoE+ EI Switch with 2 Interface Slots
```

```
MAC Address: 000f-e200-2000
```

Table 70 Command output

Field	Description
Number	ID of the device in the stack. The ID of the master is always 0.
Role	Role of the device in the stack: <ul style="list-style-type: none"> • Master—The device is the stack master. • Slave—The device is a stack member.
Sysname	Host name of the device.
MAC Address	MAC address of the device.

stack ip-pool

Syntax

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

undo stack ip-pool

View

System view

Default level

2: System level

Parameters

ip-address: Specifies the start IP address of the stack IP address pool.

mask: Specifies the IP address mask in dotted decimal notation. The system ANDs the mask with the specified IP address to identify the range of IP addresses for the stack IP address pool.

mask-length: Specifies the IP address mask in length. The system ANDs the mask with the specified IP address to identify the range of IP addresses for the stack IP address pool.

Description

Use **stack ip-pool** to configure a private IP address pool for a stack.

Use **undo stack ip-pool** to restore the default.

By default, no private IP address pool is configured for a stack.

You must configure a private IP address pool on the stack master before creating the stack. The master automatically assigns the private IP addresses in this pool to stack member devices so it can communicate with them for stack maintenance.

Make sure the number of IP addresses in the address pool is at least equal to the number of devices to be added to the stack. If not, some devices cannot join the stack for lack of private IP addresses.

Examples

Configure the IP address range from 192.168.1.1 to 192.168.1.255 for the stack private IP address pool.

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

```
[Sysname] stack ip-pool 192.168.1.1 24
```

stack role master

Syntax

stack role master

undo stack role master

View

System view

Default level

2: System level

Description

Use **stack role master** to create a stack.

Use **undo stack role master** to remove the stack.

After you execute the **stack role master** command, the device becomes a stack master device and automatically adds the devices connected to its stack ports to the stack.

You can remove the stack only on the stack master device.

Examples

Create a stack.

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

```
[Sysname] stack role master
[stack_0.Sysname]
```

stack stack-port

Syntax

```
stack stack-port stack-port-num port interface-list
undo stack stack-port stack-port-num port interface-list
```

View

System view

Default level

2: System level

Parameters

stack-port-num: Specifies the number of stack ports to be configured. The value range is 1 to 352.

interface-list: Specifies a space-separated list of Ethernet ports to be configured as stack ports. Each port is represented by its interface type and interface number. The maximum number of interfaces in the list equals the value for the *stack-port-num* argument.

Description

Use **stack stack-port** to configure stack ports on devices to be added to a stack.

Use **undo stack stack-port** to restore the default.

By default, no ports are stack ports.

Examples

```
# Configure Ethernet 1/1 as a stack port.
<Sysname> system-view
[Sysname] stack stack-port 1 ethernet 1/1
```

stack switch-to

Syntax

```
stack switch-to member-id
```

View

User view

Default level

2: System level

Parameters

member-id: Specifies the ID of a stack member. The value range depends on the device model.

Description

When you change to a stack member's CLI, your user privilege level does not change.

To return to the CLI of the stack master, use the **quit** command.

Examples

Access stack member 1 from the master device.

```
<stack_0.Sysname> stack switch-to 1
```

```
<stack_1.Sysname>
```

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](#) [C](#) [D](#) [E](#) [F](#) [H](#) [I](#) [L](#) [M](#) [N](#) [O](#) [P](#) [R](#) [S](#) [T](#) [U](#) [W](#)

A

add-member, [223](#)
administrator-address, [224](#)
advantage-factor, [117](#)
apply poe-profile, [190](#)
apply poe-profile interface, [190](#)
auto-build, [225](#)

B

black-list add-mac, [227](#)
black-list delete-mac, [228](#)
build, [228](#)

C

cluster, [230](#)
cluster enable, [230](#)
cluster switch-to, [231](#)
cluster-local-user, [232](#)
cluster-mac, [233](#)
cluster-mac syn-interval, [233](#)
cluster-snmp-agent community, [234](#)
cluster-snmp-agent group v3, [235](#)
cluster-snmp-agent mib-view, [236](#)
cluster-snmp-agent usm-user v3, [237](#)
codec-type, [117](#)

D

data-fill, [118](#)
data-size, [119](#)
debugging, [8](#)
delete-member, [238](#)
description (any NQA operation view), [120](#)
destination ip, [120](#)
destination port, [121](#)
display channel, [28](#)
display cluster, [238](#)
display cluster base-topology, [240](#)
display cluster black-list, [241](#)
display cluster candidates, [242](#)

display cluster current-topology, [243](#)
display cluster members, [245](#)
display debugging, [9](#)
display info-center, [29](#)
display ipc channel, [181](#)
display ipc link, [182](#)
display ipc multicast-group, [183](#)
display ipc node, [184](#)
display ipc packet, [184](#)
display ipc performance, [186](#)
display ipc queue, [187](#)
display logbuffer, [30](#)
display logbuffer summary, [32](#)
display mirroring-group, [107](#)
display ndp, [210](#)
display nqa history, [121](#)
display nqa reaction counters, [123](#)
display nqa result, [125](#)
display nqa server status, [168](#)
display nqa statistics, [129](#)
display ntdp, [215](#)
display ntdp device-list, [216](#)
display ntdp single-device, [218](#)
display ntp-service sessions, [11](#)
display ntp-service status, [15](#)
display ntp-service trace, [16](#)
display poe device, [191](#)
display poe interface, [192](#)
display poe interface power, [195](#)
display poe pse, [196](#)
display poe pse interface, [198](#)
display poe pse interface power, [199](#)
display poe-profile, [201](#)
display poe-profile interface, [202](#)
display rmon alarm, [90](#)
display rmon event, [91](#)
display rmon eventlog, [92](#)
display rmon history, [94](#)

- display rmon prialarm,96
- display rmon statistics,98
- display security-logfile buffer,33
- display security-logfile summary,34
- display sflow,173
- display snmp-agent community,58
- display snmp-agent group,59
- display snmp-agent local-engineid,60
- display snmp-agent mib-view,61
- display snmp-agent statistics,63
- display snmp-agent sys-info,64
- display snmp-agent trap queue,65
- display snmp-agent trap-list,66
- display snmp-agent usm-user,67
- display stack,258
- display trapbuffer,35
- Documents,263

E

- enable log updown,36
- enable snmp trap updown,68

F

- filename,135
- frequency,136
- ftp-server,248

H

- history-record enable,136
- history-record keep-time,137
- history-record number,137
- holdtime,249
- http-version,138

I

- info-center channel name,37
- info-center console channel,37
- info-center enable,38
- info-center format unicom,38
- info-center logbuffer,39
- info-center logfile overwrite-protection,40
- info-center loghost,40
- info-center loghost source,41
- info-center monitor channel,42
- info-center security-logfile alarm-threshold,43
- info-center security-logfile enable,44
- info-center security-logfile frequency,44

- info-center security-logfile size-quota,45
- info-center security-logfile switch-directory,45
- info-center snmp channel,46
- info-center source,47
- info-center synchronous,48
- info-center syslog channel,50
- info-center timestamp,50
- info-center timestamp loghost,51
- info-center trapbuffer,52
- ipc performance enable,188
- ip-pool,249

L

- logging-host,250

M

- management-vlan,251
- management-vlan synchronization enable,251
- mirroring-group,108
- mirroring-group mirroring-port,109
- mirroring-group monitor-egress,110
- mirroring-group monitor-port,111
- mirroring-group reflector-port,112
- mirroring-group remote-probe vlan,113
- mirroring-port,114
- mirror-to,116
- mode,139
- monitor-port,115

N

- ndp enable,212
- ndp timer aging,213
- ndp timer hello,214
- next-hop,139
- nm-interface vlan-interface,252
- nqa,140
- nqa agent enable,141
- nqa agent max-concurrent,141
- nqa schedule,142
- nqa server enable,169
- nqa server tcp-connect,169
- nqa server tcp-connect tos,170
- nqa server udp-echo,171
- nqa server udp-echo tos,171
- ntdp enable,220
- ntdp explore,220

- ntdp hop, [221](#)
- ntdp timer, [221](#)
- ntdp timer hop-delay, [222](#)
- ntdp timer port-delay, [223](#)
- ntp-service access, [17](#)
- ntp-service authentication enable, [18](#)
- ntp-service authentication-keyid, [19](#)
- ntp-service broadcast-client, [20](#)
- ntp-service broadcast-server, [20](#)
- ntp-service dscp, [21](#)
- ntp-service in-interface disable, [22](#)
- ntp-service max-dynamic-sessions, [22](#)
- ntp-service multicast-client, [23](#)
- ntp-service multicast-server, [24](#)
- ntp-service reliable authentication-keyid, [24](#)
- ntp-service source-interface, [25](#)
- ntp-service unicast-peer, [26](#)
- ntp-service unicast-server, [26](#)

O

- operation (FTP operation view), [143](#)
- operation (HTTP operation view), [143](#)
- operation interface, [144](#)

P

- password (FTP operation view), [144](#)
- ping, [1](#)
- ping ipv6, [4](#)
- poe disconnect, [203](#)
- poe enable, [203](#)
- poe legacy enable, [204](#)
- poe max-power, [205](#)
- poe pd-description, [205](#)
- poe pd-policy priority, [206](#)
- poe priority, [207](#)
- poe update, [208](#)
- poe utilization-threshold, [208](#)
- poe-profile, [209](#)
- probe count, [145](#)
- probe packet-interval, [146](#)
- probe packet-number, [147](#)
- probe packet-timeout, [147](#)
- probe timeout, [148](#)

R

- reaction checked-element { jitter-ds | jitter-sd }, [150](#)

- reaction checked-element { owd-ds | owd-sd }, [152](#)
- reaction checked-element icpif, [149](#)
- reaction checked-element mos, [151](#)
- reaction checked-element packet-loss, [153](#)
- reaction checked-element probe-duration, [154](#)
- reaction checked-element probe-fail (for trap), [156](#)
- reaction checked-element probe-fail (for trigger), [157](#)
- reaction checked-element rtt, [158](#)

- reaction trap, [159](#)
- reboot member, [252](#)
- reset ipc performance, [189](#)
- reset logbuffer, [53](#)
- reset ndp statistics, [214](#)
- reset trapbuffer, [53](#)
- resolve-target, [160](#)
- rmon alarm, [100](#)
- rmon event, [102](#)
- rmon history, [103](#)
- rmon prialarm, [104](#)
- rmon statistics, [106](#)
- route-option bypass-route, [160](#)

S

- security-logfile save, [54](#)
- sflow agent, [174](#)
- sflow collector, [175](#)
- sflow counter collector, [177](#)
- sflow counter interval, [176](#)
- sflow flow collector, [177](#)
- sflow flow max-header, [178](#)
- sflow sampling-mode, [178](#)
- sflow sampling-rate, [179](#)
- sflow source, [180](#)
- snmp-agent, [69](#)
- snmp-agent calculate-password, [69](#)
- snmp-agent community, [71](#)
- snmp-agent group, [72](#)
- snmp-agent ifmib long-ifindex enable, [75](#)
- snmp-agent local-engineid, [73](#)
- snmp-agent log, [74](#)
- snmp-agent mib-view, [76](#)
- snmp-agent packet max-size, [77](#)
- snmp-agent packet response dscp, [77](#)
- snmp-agent sys-info, [78](#)
- snmp-agent target-host, [79](#)

- snmp-agent trap enable, [80](#)
- snmp-agent trap if-mib link extended, [81](#)
- snmp-agent trap life, [82](#)
- snmp-agent trap queue-size, [83](#)
- snmp-agent trap source, [84](#)
- snmp-agent usm-user { v1 | v2c }, [84](#)
- snmp-agent usm-user v3, [86](#)
- snmp-host, [253](#)
- source interface, [161](#)
- source ip, [162](#)
- source port, [162](#)
- stack ip-pool, [259](#)
- stack role master, [260](#)
- stack stack-port, [261](#)
- stack switch-to, [261](#)
- statistics hold-time, [163](#)
- statistics interval, [164](#)
- statistics max-group, [163](#)
- Subscription service, [263](#)

T

- terminal debugging, [54](#)
- terminal logging, [55](#)
- terminal monitor, [56](#)
- terminal trapping, [56](#)
- tftp-server, [254](#)
- timer, [254](#)
- topology accept, [255](#)
- topology restore-from, [256](#)
- topology save-to, [256](#)
- tos, [165](#)
- tracert, [6](#)
- tracert ipv6, [7](#)
- ttl, [165](#)
- type, [166](#)

U

- url, [167](#)
- username (FTP operation view), [167](#)

W

- Websites, [263](#)