

HP Moonshot-45XGc Switch

High Availability

Command Reference

Part Number: 785515-001

Software version: ESS 2407

Document version: 5W100-20140912



Legal and notice information

© Copyright 2014 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

| | |
|--|----|
| Ethernet OAM commands | 1 |
| display oam | 1 |
| display oam configuration | 5 |
| display oam critical-event | 6 |
| display oam link-event | 7 |
| oam enable | 10 |
| oam errored-frame threshold | 11 |
| oam errored-frame window | 12 |
| oam errored-frame-period threshold | 12 |
| oam errored-frame-period window | 13 |
| oam errored-frame-seconds threshold | 14 |
| oam errored-frame-seconds window | 15 |
| oam errored-symbol-period threshold | 16 |
| oam errored-symbol-period window | 16 |
| oam global errored-frame threshold | 17 |
| oam global errored-frame window | 18 |
| oam global errored-frame-period threshold | 19 |
| oam global errored-frame-period window | 19 |
| oam global errored-frame-seconds threshold | 20 |
| oam global errored-frame-seconds window | 21 |
| oam global errored-symbol-period threshold | 22 |
| oam global errored-symbol-period window | 22 |
| oam global timer hello | 23 |
| oam global timer keepalive | 24 |
| oam mode | 25 |
| oam remote-failure action | 26 |
| oam remote-loopback | 26 |
| oam remote-loopback interface | 27 |
| oam remote-loopback reject-request | 28 |
| oam timer hello | 28 |
| oam timer keepalive | 29 |
| reset oam | 30 |
| CFD commands | 32 |
| cfd ais enable | 32 |
| cfd ais level | 32 |
| cfd ais period | 33 |
| cfd ais-track link-status global | 34 |
| cfd ais-track link-status level | 34 |
| cfd ais-track link-status period | 35 |
| cfd ais-track link-status vlan | 36 |
| cfd cc enable | 37 |
| cfd cc interval | 38 |
| cfd dm one-way | 39 |
| cfd dm two-way | 39 |
| cfd enable | 40 |
| cfd linktrace | 41 |
| cfd linktrace auto-detection | 42 |
| cfd loopback | 43 |

| | |
|--|-----------|
| cfm md | 44 |
| cfm mep | 45 |
| cfm meplist | 46 |
| cfm mip-rule | 47 |
| cfm service-instance | 48 |
| cfm slm | 49 |
| cfm tst | 50 |
| display cfm ais | 51 |
| display cfm ais-track link-status | 53 |
| display cfm dm one-way history | 54 |
| display cfm linktrace-reply | 55 |
| display cfm linktrace-reply auto-detection | 57 |
| display cfm md | 58 |
| display cfm mep | 59 |
| display cfm meplist | 62 |
| display cfm mp | 62 |
| display cfm remote-mep | 64 |
| display cfm service-instance | 65 |
| display cfm status | 66 |
| display cfm tst | 66 |
| reset cfm dm one-way history | 68 |
| reset cfm tst | 68 |
| DLDLP commands | 70 |
| display dldp | 70 |
| display dldp statistics | 71 |
| dldp authentication-mode | 73 |
| dldp authentication-password | 73 |
| dldp delaydown-timer | 74 |
| dldp enable | 75 |
| dldp global enable | 76 |
| dldp interval | 76 |
| dldp unidirectional-shutdown | 77 |
| reset dldp statistics | 78 |
| RRPP commands | 79 |
| control-vlan | 79 |
| display rrpp brief | 79 |
| display rrpp ring-group | 82 |
| display rrpp statistics | 82 |
| display rrpp verbose | 85 |
| domain ring | 88 |
| fast-detection enable | 89 |
| fast-edge-timer | 90 |
| fast-timer | 90 |
| protected-vlan | 91 |
| reset rrpp statistics | 92 |
| ring | 93 |
| ring enable | 94 |
| rrpp domain | 95 |
| rrpp enable | 96 |
| rrpp ring-group | 96 |
| timer | 97 |
| Smart Link commands | 98 |
| display smart-link flush | 98 |

| | |
|--------------------------------|------------|
| display smart-link group | 98 |
| flush enable | 100 |
| port | 100 |
| port smart-link group | 101 |
| port smart-link group track | 103 |
| preemption delay | 104 |
| preemption mode | 104 |
| protected-vlan | 105 |
| reset smart-link statistics | 106 |
| smart-link flush enable | 107 |
| smart-link group | 107 |
| Monitor Link commands | 109 |
| display monitor-link group | 109 |
| downlink up-delay | 110 |
| monitor-link group | 110 |
| port | 111 |
| port monitor-link group | 112 |
| VRRP commands | 114 |
| IPv4 VRRP commands | 114 |
| display vrrp | 114 |
| display vrrp statistics | 121 |
| reset vrrp statistics | 124 |
| snmp-agent trap enable vrrp | 125 |
| vrrp check-ttl enable | 125 |
| vrrp dscp | 126 |
| vrrp mode | 127 |
| vrrp version | 128 |
| vrrp vrid | 128 |
| vrrp vrid authentication-mode | 129 |
| vrrp vrid preempt-mode | 130 |
| vrrp vrid priority | 131 |
| vrrp vrid shutdown | 132 |
| vrrp vrid source-interface | 133 |
| vrrp vrid timer advertise | 134 |
| vrrp vrid track | 135 |
| IPv6 VRRP commands | 137 |
| display vrrp ipv6 | 137 |
| display vrrp ipv6 statistics | 144 |
| reset vrrp ipv6 statistics | 147 |
| vrrp ipv6 dscp | 147 |
| vrrp ipv6 mode | 148 |
| vrrp ipv6 vrid | 149 |
| vrrp ipv6 vrid preempt-mode | 150 |
| vrrp ipv6 vrid priority | 151 |
| vrrp ipv6 vrid shutdown | 151 |
| vrrp ipv6 vrid timer advertise | 152 |
| vrrp ipv6 vrid track | 153 |
| BFD commands | 156 |
| bfd authentication-mode | 156 |
| bfd demand enable | 157 |
| bfd detect-interface | 157 |
| bfd detect-multiplier | 158 |
| bfd echo enable | 159 |

| | |
|---|------------|
| bfd echo-source-ip | 160 |
| bfd echo-source-ipv6 | 160 |
| bfd min-echo-receive-interval | 161 |
| bfd min-receive-interval | 162 |
| bfd min-transmit-interval | 162 |
| bfd multi-hop authentication-mode | 163 |
| bfd multi-hop destination-port | 164 |
| bfd multi-hop detect-multiplier | 164 |
| bfd multi-hop min-receive-interval | 165 |
| bfd multi-hop min-transmit-interval | 166 |
| bfd session init-mode | 167 |
| bfd template | 167 |
| display bfd session | 168 |
| reset bfd session statistics | 170 |
| Track commands | 172 |
| display track | 172 |
| track bfd | 174 |
| track cfd | 175 |
| track interface | 176 |
| track interface protocol | 177 |
| track nqa | 178 |
| Process placement commands | 180 |
| affinity location-set | 180 |
| affinity location-type | 181 |
| affinity program | 181 |
| affinity self | 182 |
| display ha service-group | 183 |
| display placement location | 185 |
| display placement policy | 185 |
| display placement program | 186 |
| display placement reoptimize | 187 |
| placement program | 188 |
| placement reoptimize | 189 |
| Index | 191 |

Ethernet OAM commands

display oam

Use **display oam** to display the information about an Ethernet OAM connection, including connection status, information contained in Ethernet OAM packet header, and Ethernet OAM packet statistics.

Syntax

```
display oam { local | remote } [ interface interface-type interface-number ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

local: Displays the Ethernet OAM connection information of the local end.

remote: Displays the Ethernet OAM connection information of the remote end.

interface *interface-type interface-number*: Specifies a port by its type and number.

Usage guidelines

If you do not specify the **interface** keyword, the command displays information about all the Ethernet OAM connections.

Examples

```
# Display information about the Ethernet OAM connection established on all local ports.
```

```
<Sysname> display oam local  
----- [FortyGigE1/1/1] -----  
Enable status      : Enable  
Loopback status   : No loopback  
Link status       : UP  
OAM mode          : Active  
PDU               : ANY  
Mux action        : FWD  
Par action        : FWD
```

```
# Display information about the Ethernet OAM connection established on the local port FortyGigE  
1/1/1.
```

```
<Sysname> display oam local interface fortygige 1/1/1  
Enable status      : Enable  
Loopback status   : No loopback  
Link status       : UP  
OAM mode          : Active  
PDU               : ANY
```

```

Mux action      : FWD
Par action      : FWD
Flags
  Link fault    : Not occurred
  Dying gasp    : Not occurred
  Critical event : Not occurred
  Local evaluating : COMPLETE
  Remote evaluating : COMPLETE
Packets statistics
  Packet type          Sent          Received
  -----
  OAMPDU              100          80
  OAMInformation       64           60
  OAMEventNotification 36           20
  OAMUniqueEventNotification 36          10
  OAMDuplicateEventNotification 0           10

```

Table 1 Command output

| Field | Description |
|-----------------|---|
| FortyGigE1/1/1 | Information on FortyGigE 1/1/1. |
| Enable status | Ethernet OAM state (enabled or disabled). |
| Loopback status | Ethernet OAM loopback state: <ul style="list-style-type: none"> No loopback. Remote loopback. Local loopback. |
| Link status | Link state (UP or DOWN). |
| OAM mode | Local Ethernet OAM mode: <ul style="list-style-type: none"> Active—The port operates in the active Ethernet OAM mode. Passive—The port operates in the passive Ethernet OAM mode. |
| PDU | The way in which the local end processes Ethernet OAMPDUs: <ul style="list-style-type: none"> RX_INFO—The port only receives Information OAMPDUs and does not send any Ethernet OAMPDUs. LF_INFO—The port only sends the Information OAMPDUs without Information TLV triplets and with their link error flag bits being set. INFO—The port sends and receives only Information OAMPDUs. ANY—The port sends and receives Ethernet OAMPDUs of any type. |
| Mux action | Operating mode of the local transmitter: <ul style="list-style-type: none"> FWD—The port can send any packets. DISCARD—The port only sends Ethernet OAMPDUs. |
| Par action | Operating mode of the local receiver: <ul style="list-style-type: none"> FWD—The port can receive any packets. DISCARD—The port only receives Ethernet OAMPDUs. LB—The local receiver is in loopback state. All the packets, other than Ethernet OAMPDUs, received on the local receiver are returned to their sources along their original routes. |

| Field | Description |
|-------------------------------|--|
| Flags | Local flags inserted in the local flag fields of the Ethernet OAMPDUs sent. |
| Link fault | Indicates whether an Ethernet OAM link error is present. |
| Dying gasp | Indicates whether a fatal error is present. |
| Critical event | Indicates whether a critical error is present. |
| Local evaluating | Indicates whether the local-to-remote configuration negotiation is complete: <ul style="list-style-type: none"> • COMPLETE—The negotiation is completed. • NOTCOMPLETE—The negotiation is uncompleted. |
| Remote evaluating | Indicates whether the remote-to-local configuration negotiation is complete: <ul style="list-style-type: none"> • COMPLETE—The negotiation is completed. • NOTCOMPLETE—The negotiation is uncompleted. • RESERVED—The field is reserved and the negotiation is uncompleted. • UNSATISFIED—The remote end is not satisfied with the local configuration and the negotiation is uncompleted. |
| Packets statistics | Statistics about Ethernet OAMPDUs sent and received. |
| OAMPDU | Total number of the Ethernet OAMPDUs sent and received. |
| OAMInformation | Number of the Information OAMPDUs sent and received. |
| OAMEventNotification | Number of the Event notification OAMPDUs sent and received. |
| OAMUniqueEventNotification | Number of the unduplicated Event notification OAMPDUs sent or received uniquely. |
| OAMDuplicateEventNotification | Number of the duplicate Event notification OAMPDUs sent or received. |

Display the Ethernet OAM information about all remote ports.

```
<Sysname> display oam remote
----- [FortyGigE1/1/1] -----
OAM mode           : Active
MAC address        : 3822-d6a2-a800
MTU size           : 1500
Mux action         : FWD
Par action         : FWD
```

Display the Ethernet OAM information about the peer port FortyGigE 1/1/1.

```
<Sysname> display oam remote interface fortygige 1/1/1
OAM mode           : Active
MAC address        : 3822-d6a2-a800
MTU size           : 1500
Mux action         : FWD
Par action         : FWD
Configuration
  Unidirectional   : Not supported
  Remote loopback  : Supported
  Link events      : Supported
  MIB retrieval    : Not supported
Flags
  Link fault       : Not occurred
```

Dying gasp : Not occurred
 Critical event : Not occurred
 Local evaluating : COMPLETE
 Remote evaluating : COMPLETE

Table 2 Command output

| Field | Description |
|------------------|--|
| FortyGigE1/1/1 | Information on FortyGigE 1/1/1. |
| OAM mode | Local Ethernet OAM mode: <ul style="list-style-type: none"> • Active—The port operates in the active Ethernet OAM mode. • Passive—The port operates in the passive Ethernet OAM mode. |
| MAC address | MAC address of the remote end. |
| MTU size | MTU size, in bytes. |
| Mux action | Operating mode of the remote transmitter: <ul style="list-style-type: none"> • FWD—The port can send any packets. • DISCARD—The port only sends Ethernet OAMPDUs. |
| Par action | Operating mode of the remote receiver: <ul style="list-style-type: none"> • FWD—The port can receive any packets. • DISCARD—The port only receives Ethernet OAMPDUs. • LB—The local receiver is in loopback state. All the packets, other than Ethernet OAMPDUs, received on the local receiver are returned to their sources along their original routes. |
| Configuration | Configuration of the remote Ethernet OAM entity. |
| Unidirectional | Indicates whether unidirectional transmission is supported. |
| Remote loopback | Indicates whether Ethernet OAM remote loopback is supported. |
| Link events | Indicates whether Ethernet OAM link error events are supported. |
| MIB retrieval | Indicates whether MIB variable retrieval is supported. |
| Flags | Values of the peer Ethernet OAM flag fields in OAM packets. |
| Link fault | Indicates whether an Ethernet OAM link error is present. |
| Dying gasp | Indicates whether a fatal error is present. |
| Critical event | Indicates whether a critical error is present. |
| Local evaluating | Indicates whether the local-to-remote configuration negotiation is complete: <ul style="list-style-type: none"> • COMPLETE—The negotiation is completed. • NOTCOMPLETE—The negotiation is uncompleted. • RESERVED—The field is reserved and the negotiation is uncompleted. • UNSATISFIED—The remote end is not satisfied with the local configuration and the negotiation is uncompleted. |

| Field | Description |
|-------------------|--|
| Remote evaluating | <p>Indicates whether the remote-to-local configuration negotiation is complete:</p> <ul style="list-style-type: none"> • COMPLETE—The negotiation is completed. • NOTCOMPLETE—The negotiation is uncompleted. • UNSATISFIED—The remote end is not satisfied with the local configuration and the negotiation is uncompleted. |

Related commands

reset oam

display oam configuration

Use **display oam configuration** to display global Ethernet OAM configuration on the specified port, including the periods and thresholds for Ethernet OAM link error event detection.

Syntax

display oam configuration [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

Usage guidelines

If you do not specify the **interface** keyword, the command displays Ethernet OAM configuration globally and on ports that do not use the default configuration.

Examples

Display Ethernet OAM configuration globally and on ports that do not use the default configuration.

```
<Sysname> display oam configuration
----- [Global] -----
OAM timers
  Hello timer      : 1000 milliseconds
  Keepalive timer  : 5000 milliseconds
Link monitoring
  Errored symbol period
    Window         : 100 x 1000000 symbols
    Threshold       : 1 error symbols
  Errored frame
    Window         : 10 x 100 milliseconds
    Threshold       : 1 error frames
  Errored frame period
    Window         : 1000 x 10000 frames
```

```

Threshold          : 1 error frames
Errored frame seconds
Window            : 600 x 100 milliseconds
Threshold        : 1 error seconds

----- [FortyGigE1/1/1] -----
OAM timers
Hello timer       : 500 milliseconds
Keepalive timer   : 5000 milliseconds
Link monitoring
Errored symbol period
Window            : 100 x 1000000 symbols
Threshold        : 1 error symbols
Errored frame
Window            : 10 x 100 milliseconds
Threshold        : 1 error frames
Errored frame period
Window            : 1000 x 10000 frames
Threshold        : 1 error frames
Errored frame seconds
Window            : 600 x 100 milliseconds
Threshold        : 1 error seconds

```

Table 3 Command output

| Field | Description |
|-----------------------|--|
| Global | Global information. |
| FortyGigE1/1/1 | Information on FortyGigE 1/1/1. |
| OAM timers | Ethernet OAM connection detection timers. |
| Hello timer | Ethernet OAM handshake packet transmission interval. |
| Keepalive timer | Ethernet OAM connection timeout timer. |
| Link monitoring | Link event detection window and threshold. |
| Errored symbol period | Errored symbol event. |
| Errored frame | Errored frame event. |
| Errored frame period | Errored frame period event. |
| Errored frame seconds | Errored frame seconds event. |
| Window | Detection window configured for link events. |
| Threshold | Triggering threshold configured for link events. |

display oam critical-event

Use **display oam critical-event** to display the statistics of critical Ethernet OAM link events that occurred on a port.

Syntax

display oam critical-event [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

Usage guidelines

If you do not specify the **interface** keyword, the command displays the statistics of the critical Ethernet OAM link events that occurred on all the ports of the switch.

Examples

Display the statistics of critical Ethernet OAM link events that occurred on all the ports.

```
<Sysname> display oam critical-event
----- [FortyGigE1/1/1] -----
Local link status      : UP
Event statistics
  Link fault           : Not occurred
  Dying gasp           : Not occurred
  Critical event       : Not occurred
```

Table 4 Command output

| Field | Description |
|-------------------|--|
| FortyGigE1/1/1 | Information on FortyGigE 1/1/1. |
| Local link status | Local link status, up or down. |
| Event statistics | Statistics of critical Ethernet OAM link events. |
| Link fault | Indicates whether a link fault is present. |
| Dying Gasp | Indicates whether a fatal fault is present. |
| Critical Event | Indicates whether a critical fault is present. |

display oam link-event

Use **display oam link-event** to display the statistics of Ethernet OAM link error events that occurred on a local port or a peer port. Ethernet OAM link error events include errored symbol events, errored frame events, errored frame period events, and errored frame seconds events.

Syntax

display oam link-event { **local** | **remote** } [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

local: Displays the statistics on the local Ethernet OAM link error events.

remote: Displays the statistics on the peer Ethernet OAM link error events.

interface *interface-type interface-number*: Specifies a port by its type and number.

Usage guidelines

If you do not specify the **interface** keyword, the command displays the statistics of the Ethernet OAM link error events that occurred on all the local/peer ports.

Examples

Display the statistics of Ethernet OAM link error events that occurred on all the local ports.

```
<Sysname> display oam link-event local
----- [FortyGigE1/1/1] -----
Link status: UP
OAM local errored frame event
  Event time stamp      : 49582 x 100 milliseconds
  Errored frame window  : 10 x 100 milliseconds
  Errored frame threshold : 1 error frames
  Errored frame         : 1 error frames
  Error running total   : 6 error frames
  Event running total   : 6 events
OAM local errored frame period event
  Event time stamp      : 16382 x 100 milliseconds
  Errored frame period window : 10000000 frames
  Errored frame period threshold : 1 error frames
  Errored frame period   : 1 error frames
  Error running total   : 5 error frames
  Event running total   : 5 events
OAM local errored frame seconds summary event
  Event time stamp      : 50022 x 100 milliseconds
  Errored frame seconds window : 600 x 100 milliseconds
  Errored frame seconds threshold : 1 error seconds
  Errored frame seconds   : 1 error seconds
  Error running total   : 1 error seconds
  Event running total   : 1 events
```

Display Ethernet OAM link event statistics of the remote ends of all the ports.

```
<Sysname> display oam link-event remote
----- [FortyGigE1/1/1] -----
Link status: UP
OAM remote errored symbol event
  Event time stamp      : 35498 x 100 milliseconds
  Errored symbol window : 100000000 symbols
  Errored symbol threshold : 1 error symbols
  Errored symbol        : 1 error symbols
```

```

Error running total      : 4 error symbols
Event running total     : 4 events
OAM remote errored frame event
Event time stamp        : 49582 x 100 milliseconds
Errored frame window    : 10 x 100 milliseconds
Errored frame threshold : 1 error frames
Errored frame           : 1 error frames
Error running total     : 6 error frames
Event running total     : 6 events
OAM remote errored frame period event
Event time stamp        : 16382 x 100 milliseconds
Errored frame period window : 10000000 frames
Errored frame period threshold : 1 error frames
Errored frame period    : 1 error frames
Error running total     : 5 error frames
Event running total     : 5 events
OAM remote errored frame seconds summary event
Event time stamp        : 50022 x 100 milliseconds
Errored frame seconds window : 600 x 100 milliseconds
Errored frame seconds threshold : 1 error seconds
Errored frame seconds   : 1 error seconds
Error running total     : 1 error seconds
Event running total     : 1 events

```

Table 5 Command output

| Field | Description |
|---------------------------------|--|
| FortyGigE1/1/1 | Information on FortyGigE 1/1/1. |
| Link status | Link status, up or down. |
| OAM remote errored symbol event | <p>Information about remote errored symbol events (available only when remote errored symbol events occur):</p> <ul style="list-style-type: none"> • Event time stamp—Time when an errored symbol event occurred. • Errored symbol window—Errored symbol detection interval. • Errored symbol threshold—Errored threshold that triggers an errored symbol event. • Errored symbol—Number of detected errored symbols in the most recent errored symbol event. • Error running total—Total number of errored symbols. • Event running total—Total number of errored symbol events that have occurred. |

| Field | Description |
|--|--|
| OAM local/remote errored frame event | <p>Information about local/remote end errored frame events (available only when local/remote end errored frame events occur):</p> <ul style="list-style-type: none"> • Event time stamp—Time when an errored frame event occurred. • Errored frame window—Errored frame detection interval. • Errored frame threshold—Errored threshold that triggers an errored frame event. • Errored frame—Number of detected errored frames in the most recent errored frame event. • Error running total—Total number of errored frames. • Event running total—Total number of errored frame events that have occurred. |
| OAM local/remote errored frame period event | <p>Information about local/remote errored frame period events (available only when local/remote errored frame period events occur):</p> <ul style="list-style-type: none"> • Event time stamp—Time when an errored frame period event occurred. • Errored frame period window—Errored frame period detection interval. • Errored frame period threshold—Errored threshold that triggers an errored frame period event. • Errored frame period—Number of detected errored frames in the most recent errored frame period event. • Error running total—Total number of errored frames that have detected. • Event running total—Total number of errored frame period events. |
| OAM local/remote errored frame seconds summary event | <p>Information about local/remote end errored frame seconds events (available only when local/remote end errored frame seconds events occur):</p> <ul style="list-style-type: none"> • Event time stamp—Time when an errored frame seconds event occurred. • Errored frame second window—Errored frame second detection interval. • Errored Frame seconds threshold—Errored threshold that triggers an errored frame seconds event. • Errored frame seconds—Number of detected errored frame seconds in the most recent errored frame seconds event. • Error running total—Total number of errored frame seconds. • Event running total—Total number of errored frame seconds events that have occurred. |

Related commands

reset oam

oam enable

Use **oam enable** to enable Ethernet OAM.

Use **undo oam enable** to disable Ethernet OAM.

Syntax

oam enable

undo oam enable

Default

Ethernet OAM is disabled.

Views

Layer 2 Ethernet port view, Layer 3 Ethernet port view

Predefined user roles

network-admin

Examples

```
# Enable OAM on FortyGigE 1/1/1.
<Sysname> system-view
[Sysname] interface fortygige 1/1/1
[Sysname-FortyGigE1/1/1] oam enable
```

oam errored-frame threshold

Use **oam errored-frame threshold** to set the errored frame event triggering threshold for a port.

Use **undo oam errored-frame threshold** to restore the default.

Syntax

oam errored-frame threshold *threshold-value*

undo oam errored-frame threshold

Default

The port uses the global setting.

Views

Layer 2 Ethernet port view, Layer 3 Ethernet port view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the errored frame event triggering threshold in number of errored frame seconds, in the range of 0 to 4294967295.

Usage guidelines

The configuration in port view takes effect on the specified port. For a port, the configuration in port view takes precedence.

Examples

```
# Set the errored frame event triggering threshold to 100.
<Sysname> system-view
[Sysname] interface fortygige 1/1/1
[Sysname-FortyGigE1/1/1] oam errored-frame threshold 100
```

Related commands

- **display oam configuration**
- **display oam link-event**

- **oam global errored-frame threshold**

oam errored-frame window

Use **oam errored-frame window** to set the errored frame event detection window.

Use **undo oam errored-frame window** to restore the default.

Syntax

oam errored-frame window *window-value*

undo oam errored-frame window

Default

The port uses the global setting.

Views

Layer 2 Ethernet port view, Layer 3 Ethernet port view

Predefined user roles

network-admin

Parameters

window-value: Specifies the errored frame event detection window in the range of 10 to 600 and in steps of 10 (in 100 milliseconds).

Usage guidelines

The configuration in port view takes effect on the specified port. For a port, the configuration in port view takes precedence.

Examples

```
# Set the errored frame event detection window on FortyGigE 1/1/1 to 2000 milliseconds.
```

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

```
[Sysname] interface fortygige 1/1/1
```

```
[Sysname-FortyGigE1/1/1] oam errored-frame window 20
```

Related commands

- **display oam configuration**
- **display oam link-event**
- **oam global errored-frame window**

oam errored-frame-period threshold

Use **oam errored-frame-period threshold** to set the errored frame period event triggering threshold on a port.

Use **undo oam errored-frame-period threshold** to restore the default.

Syntax

oam errored-frame-period threshold *threshold-value*

undo oam errored-frame-period threshold

Default

The port uses the global setting.

Views

Layer 2 Ethernet port view, Layer 3 Ethernet port view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the errored frame period event triggering threshold in the range of 0 to 4294967295.

Usage guidelines

The configuration in port view takes effect on the specified port. For a port, the configuration in port view takes precedence.

Examples

```
# Set the errored frame period event triggering threshold on FortyGigE 1/1/1 to 100.
<Sysname> system-view
[Sysname] interface fortygige 1/1/1
[Sysname-FortyGigE1/1/1] oam errored-frame-period threshold 100
```

Related commands

- **display oam configuration**
- **display oam link-event**
- **oam global errored-frame-period threshold**

oam errored-frame-period window

Use **oam errored-frame-period window** to set the errored frame period event detection window.

Use **undo oam errored-frame-period window** to restore the default.

Syntax

oam errored-frame-period window *window-value*

undo oam errored-frame-period window

Default

The port uses the global setting.

Views

Layer 2 Ethernet port view, Layer 3 Ethernet port view

Predefined user roles

network-admin

Parameters

window-value: Specifies the errored frame period event detection window in the range of 1 to 65535. The value of this argument must be a multiple of 10000.

Usage guidelines

The configuration in port view takes effect on the specified port. For a port, the configuration in port view takes precedence.

Examples

```
# Set the errored frame period event detection window to 20000000.
<Sysname> system-view
[Sysname] interface fortygige 1/1/1
[Sysname-FortyGigE1/1/1] oam errored-frame-period window 2000
```

Related commands

- **display oam configuration**
- **display oam link-event**
- **oam global errored-frame-period window**

oam errored-frame-seconds threshold

Use **oam errored-frame-seconds threshold** to set the errored frame seconds event triggering threshold on a port.

Use **undo oam errored-frame-seconds threshold** to restore the default.

Syntax

oam errored-frame-seconds threshold *threshold-value*

undo oam errored-frame-seconds threshold

Default

The port uses the global setting.

Views

Layer 2 Ethernet port view, Layer 3 Ethernet port view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the errored frame seconds event triggering threshold in the range of 0 to 900.

Usage guidelines

The value of the errored frame seconds event triggering threshold cannot be greater than the value of the errored frame seconds event detection window (in seconds). Otherwise, errored frame seconds events cannot be generated.

The configuration in port view takes effect on the specified port. For a port, the configuration in port view takes precedence.

Examples

```
# Set the errored frame seconds event triggering threshold on FortyGigE 1/1/1 to 100.
<Sysname> system-view
[Sysname] interface fortygige 1/1/1
[Sysname-FortyGigE1/1/1] oam errored-frame-seconds threshold 100
```

Related commands

- **display oam configuration**
- **display oam link-event**
- **oam errored-frame-seconds window**
- **oam global errored-frame-seconds threshold**

oam errored-frame-seconds window

Use **oam errored-frame-seconds window** to set the errored frame seconds event detection window.

Use **undo oam errored-frame-seconds window** to restore the default.

Syntax

oam errored-frame-seconds window *window-value*

undo oam errored-frame-seconds window

Default

The port uses the global setting.

Views

Layer 2 Ethernet port view, Layer 3 Ethernet port view

Predefined user roles

network-admin

Parameters

window-value: Specifies the errored frame seconds event detection window in the range of 100 to 9000 and in steps of 10 (in 100 milliseconds).

Usage guidelines

The value of the errored frame seconds event triggering threshold cannot be greater than the value of the errored frame seconds event detection window (in seconds). Otherwise, errored frame seconds events cannot be generated.

The configuration in port view takes effect on the specified port. For a port, the configuration in port view takes precedence.

Examples

```
# Set the errored frame seconds event detection window to 10000 milliseconds.
```

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

```
[Sysname] interface fortygige 1/1/1
```

```
[Sysname-FortyGigE1/1/1] oam errored-frame-seconds window 100
```

Related commands

- **display oam configuration**
- **display oam link-event**
- **oam errored-frame-seconds threshold**
- **oam errored-frame-seconds period**

oam errored-symbol-period threshold

Use **oam errored-symbol-period threshold** to set the errored symbol event triggering threshold.

Use **undo oam errored-symbol-period threshold** to restore the default.

Syntax

oam errored-symbol-period threshold *threshold-value*

undo oam errored-symbol-period threshold

Default

The port uses the global setting.

Views

Layer 2 Ethernet port view, Layer 3 Ethernet port view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the errored symbol event triggering threshold in the range of 0 to 4294967295.

Usage guidelines

The configuration in port view takes effect on the specified port. For a port, the configuration in port view takes precedence.

Examples

```
# Set the errored symbol event triggering threshold to 100.
<Sysname> system-view
[Sysname] interface fortygige 1/1/1
[Sysname-FortyGigE1/1/1] oam errored-symbol-period threshold 100
```

Related commands

- **display oam configuration**
- **display oam link-event**
- **oam global errored-symbol-period threshold**

oam errored-symbol-period window

Use **oam errored-symbol-period window** to set the errored symbol event detection window.

Use **undo oam errored-symbol-period window** to restore the default.

Syntax

oam errored-symbol-period window *window-value*

undo oam errored-symbol-period window

Default

The port uses the global setting.

Views

Layer 2 Ethernet port view, Layer 3 Ethernet port view

Predefined user roles

network-admin

Parameters

window-value: Specifies the errored symbol event detection window in the range of 1 to 65535. The value of this argument must be a multiple of 1000000.

Usage guidelines

The configuration in port view takes effect on the specified port. For a port, the configuration in port view takes precedence.

Examples

```
# Set the errored symbol event detection window on FortyGigE 1/1/1 to 200000000.  
<Sysname> system-view  
[Sysname] interface fortygige 1/1/1  
[Sysname-FortyGigE1/1/1] oam errored-symbol-period window 200
```

Related commands

- **display oam configuration**
- **display oam link-event**
- **oam global errored-symbol-period window**

oam global errored-frame threshold

Use **oam global errored-frame threshold** to set the global errored frame event triggering threshold.

Use **undo oam global errored-frame threshold** to restore the default.

Syntax

oam global errored-frame threshold *threshold-value*

undo oam global errored-frame threshold

Default

The errored frame event triggering threshold is 1.

Views

System view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the errored frame event triggering threshold in the range of 0 to 4294967295.

Usage guidelines

The configuration in system view takes effect on all ports, but has a lower precedence than the configuration in port view.

Examples

```
# Set the errored frame event triggering threshold to 100.  
<Sysname> system-view  
[Sysname] oam global errored-frame threshold 100
```

Related commands

- **display oam configuration**
- **display oam link-event**
- **oam errored-frame threshold**

oam global errored-frame window

Use **oam global errored-frame window** to set the global errored frame event detection window.

Use **undo oam global errored-frame window** to restore the default.

Syntax

```
oam global errored-frame window window-value
```

```
undo oam global errored-frame window
```

Default

The global errored frame event detection window is 1000 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

window-value: Specifies the errored frame event detection window in the range of 10 to 600 and in steps of 10 (in 100 milliseconds).

Usage guidelines

The configuration in system view takes effect on all ports, but has a lower precedence than the configuration in port view.

Examples

```
# Set the errored frame event detection window to 2000 milliseconds.  
<Sysname> system-view  
[Sysname] oam global errored-frame window 20
```

Related commands

- **display oam configuration**
- **display oam link-event**
- **oam errored-frame window**

oam global errored-frame-period threshold

Use **oam global errored-frame-period threshold** to set the global errored frame period event triggering threshold.

Use **undo oam global errored-frame-period threshold** to restore the default.

Syntax

oam global errored-frame-period threshold *threshold-value*

undo oam global errored-frame-period threshold

Default

The errored frame period event triggering threshold is 1.

Views

System view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the errored frame period event triggering threshold in the range of 0 to 4294967295.

Usage guidelines

The configuration in system view takes effect on all ports, but has a lower precedence than the configuration in port view.

Examples

```
# Set the errored frame period event triggering threshold to 100.  
<Sysname> system-view  
[Sysname] oam global errored-frame-period threshold 100
```

Related commands

- **display oam configuration**
- **display oam link-event**
- **oam errored-frame-period threshold**

oam global errored-frame-period window

Use **oam global errored-frame-period window** to set the global errored frame period event detection window.

Use **undo oam global errored-frame-period window** to restore the default.

Syntax

oam global errored-frame-period window *window-value*

undo oam global errored-frame-period window

Default

The global errored frame period event detection window is 10000000.

Views

System view

Predefined user roles

network-admin

Parameters

window-value: Specifies the errored frame period event detection window in the range of 1 to 65535. The value of this argument must be a multiple of 10000.

Usage guidelines

The configuration in system view takes effect on all ports, but has a lower precedence than the configuration in port view.

Examples

```
# Set the errored frame period event detection window to 20000000.
<Sysname> system-view
[Sysname] oam global errored-frame-period window 2000
```

Related commands

- **display oam configuration**
- **display oam link-event**
- **oam errored-frame-period window**

oam global errored-frame-seconds threshold

Use **oam global errored-frame-seconds threshold** to set the global errored frame seconds event triggering threshold.

Use **undo oam global errored-frame-seconds threshold** to restore the default.

Syntax

oam global errored-frame-seconds threshold *threshold-value*

undo oam global errored-frame-seconds threshold

Default

The global errored frame seconds event detection interval is 1.

Views

System view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the errored frame seconds event triggering threshold in the range of 0 to 900.

Usage guidelines

The value of the errored frame seconds event triggering threshold cannot be greater than the value of the errored frame seconds event detection window (in seconds). Otherwise, errored frame seconds events cannot be generated.

The configuration in system view takes effect on all ports, but has a lower precedence than the configuration in port view.

Examples

```
# Set the errored frame seconds event triggering threshold to 100.
<Sysname> system-view
[Sysname] oam global errored-frame-seconds threshold 100
```

Related commands

- **display oam configuration**
- **display oam link-event**
- **oam errored-frame-seconds threshold**
- **oam global errored-frame-seconds window**

oam global errored-frame-seconds window

Use **oam global errored-frame-seconds window** to set the global errored frame seconds event detection window.

Use **undo oam global errored-frame-seconds window** to restore the default.

Syntax

```
oam global errored-frame-seconds window window-value
undo oam global errored-frame-seconds window
```

Default

The global errored frame seconds event detection window is 60000 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

window-value: Specifies the errored frame seconds event detection window in the range of 100 to 9000 and in steps of 10 (in 100 milliseconds).

Usage guidelines

The value of the errored frame seconds event triggering threshold cannot be greater than the value of the errored frame seconds event detection window (in seconds). Otherwise, errored frame seconds events cannot be generated.

The configuration in system view takes effect on all ports, but has a lower precedence than the configuration in port view.

Examples

```
# Set the errored frame seconds event detection window to 10000 milliseconds.
<Sysname> system-view
[Sysname] oam global errored-frame-seconds window 100
```

Related commands

- **display oam configuration**
- **display oam link-event**
- **oam errored-frame-seconds period**
- **oam global errored-frame-seconds threshold**

oam global errored-symbol-period threshold

Use **oam global errored-symbol-period threshold** to set the global errored symbol event triggering threshold.

Use **undo oam global errored-symbol-period threshold** to restore the default.

Syntax

oam global errored-symbol-period threshold *threshold-value*

undo oam global errored-symbol-period threshold

Default

The global errored symbol event triggering threshold is 1.

Views

System view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the errored symbol event triggering threshold in the range of 0 to 4294967295.

Usage guidelines

The configuration in system view takes effect on all ports, but has a lower precedence than the configuration in port view.

Examples

```
# Set the errored symbol event triggering threshold to 100.
<Sysname> system-view
[Sysname] oam global errored-symbol-period threshold 100
```

Related commands

- **display oam configuration**
- **display oam link-event**
- **oam errored-symbol-period threshold**

oam global errored-symbol-period window

Use **oam global errored-symbol-period window** to set the global errored symbol event detection window.

Use **undo oam global errored-symbol-period window** to restore the default.

Syntax

```
oam global errored-symbol-period window window-value  
undo oam global errored-symbol-period window
```

Default

The global errored symbol event detection window is 100000000.

Views

System view

Predefined user roles

network-admin

Parameters

window-value: Specifies the errored symbol event detection window in the range of 1 to 65535. The value of this argument must be a multiple of 1000000.

Usage guidelines

The configuration in system view takes effect on all ports, but has a lower precedence than the configuration in port view.

Examples

```
# Set the errored symbol event detection window to 200000000.  
<Sysname> system-view  
[Sysname] oam global errored-symbol-period window 200
```

Related commands

- **display oam configuration**
- **display oam link-event**
- **oam global errored-symbol-period window**

oam global timer hello

Use **oam global timer hello** to configure the global Ethernet OAM handshake packet transmission interval.

Use **undo oam global timer hello** to restore the default.

Syntax

```
oam global timer hello interval  
undo oam global timer hello
```

Default

The global Ethernet OAM handshake packet transmission interval is 1000 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the Ethernet OAM handshake packet transmission interval, in steps of 100 (in milliseconds). The value range for this argument is 500 to 5000.

Usage guidelines

After the timeout timer of an Ethernet OAM connection expires, the local OAM entity ages out its connection with the peer OAM entity, causing the OAM connection to disconnect. To keep the Ethernet OAM connections stable, HP recommends that you set the connection timeout timer to be at least five times the handshake packet transmission interval.

The configuration in system view takes effect on all ports, but has a lower precedence than the configuration in port view.

Examples

```
# Set the Ethernet OAM handshake packet transmission interval to 600 milliseconds.
<Sysname> system-view
[Sysname] oam global timer hello 600
```

Related commands

- **display oam configuration**
- **oam timer hello**

oam global timer keepalive

Use **oam global timer keepalive** to configure the global Ethernet OAM connection timeout timer.

Use **undo oam global timer keepalive** to restore the default.

Syntax

```
oam global timer keepalive interval
undo oam global timer keepalive
```

Default

The global Ethernet OAM connection timeout timer is 5000 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the Ethernet OAM connection timeout timer, in steps of 100 (in milliseconds). The value range for this argument is 1000 to 25000.

Usage guidelines

After the timeout timer of an Ethernet OAM connection expires, the local OAM entity ages out its connection with the peer OAM entity, causing the OAM connection to disconnect. To keep the Ethernet OAM connections stable, HP recommends that you set the connection timeout timer to be at least five times the handshake packet transmission interval.

The configuration in system view takes effect on all ports, but has a lower precedence than the configuration in port view.

Examples

```
# Set the Ethernet OAM connection timeout timer to 6000 milliseconds.
<Sysname> system-view
[Sysname] oam global timer keepalive 6000
```

Related commands

- **display oam configuration**
- **oam timer keepalive**

oam mode

Use **oam mode** to set the Ethernet OAM mode.

Use **undo oam mode** to restore the default.

Syntax

```
oam mode { active | passive }
undo oam mode
```

Default

An Ethernet OAM-enabled Ethernet port operates in the active Ethernet OAM mode.

Views

Layer 2 Ethernet port view, Layer 3 Ethernet port view

Predefined user roles

network-admin

Parameters

active: Specifies the active Ethernet OAM mode.

passive: Specifies the passive Ethernet OAM mode.

Usage guidelines

To change the Ethernet OAM mode of an Ethernet OAM-enabled Ethernet port, first disable Ethernet OAM on the port.

Examples

```
# Disable Ethernet OAM on FortyGigE 1/1/1, and then configure FortyGigE 1/1/1 to operate in
passive Ethernet OAM mode.
<Sysname> system-view
[Sysname] interface fortygige 1/1/1
[Sysname-FortyGigE1/1/1] undo oam enable
[Sysname-FortyGigE1/1/1] oam mode passive
```

Related commands

oam enable

oam remote-failure action

Use **oam remote-failure action** to configure the action the port takes after it receives an Ethernet OAM event from the remote end.

Use **undo oam remote-failure action** to restore the default.

Syntax

```
oam remote-failure { connection-expired | critical-event | dying-gasp | link-fault } action error-link-down
```

```
undo oam remote-failure { connection-expired | critical-event | dying-gasp | link-fault } action error-link-down
```

Default

The port only logs the Ethernet OAM event it receives from the remote end.

Views

Layer 2 Ethernet port view, Layer 3 Ethernet port view

Predefined user roles

network-admin

Parameters

connection-expired: Specifies a connection timeout fault.

critical-event: Specifies a critical fault.

dying-gasp: Specifies a fatal fault.

link-fault: Specifies a link fault.

error-link-down: Terminates the OAM connection, and sets the link state of the port to down.

Examples

```
# Configure FortyGigE 1/1/1 to terminate the OAM connection after it receives a fatal fault from the remote end, and set the link state of the port to down.
```

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

```
[Sysname] interface fortygige 1/1/1
```

```
[Sysname-FortyGigE1/1/1] oam remote-failure dying-gasp action error-link-down
```

oam remote-loopback

Use **oam remote-loopback start** to enable Ethernet OAM remote loopback on the specified Ethernet port.

Use **oam remote-loopback stop** to disable Ethernet OAM remote loopback on the Ethernet port.

Syntax

```
oam remote-loopback start
```

```
oam remote-loopback stop
```

Default

Ethernet OAM remote loopback is disabled on the Ethernet port.

Views

Layer 2 Ethernet port view, Layer 3 Ethernet port view

Predefined user roles

network-admin

Usage guidelines

Ethernet OAM remote loopback is available only after the Ethernet OAM connection is established and can be performed only by the Ethernet OAM entities operating in active Ethernet OAM mode.

You can enable Ethernet OAM remote loopback on a specified port in user view or system view, or enable it on the current port in port view. The configurations have the same effect.

Examples

Configure the active Ethernet OAM mode and enable Ethernet OAM on FortyGigE 1/1/1, and then enable Ethernet OAM remote loopback on FortyGigE 1/1/1 in Layer 2 Ethernet port view.

```
<Sysname> system-view
[Sysname] interface fortygige 1/1/1
[Sysname-FortyGigE1/1/1] oam mode active
[Sysname-FortyGigE1/1/1] oam enable
[Sysname-FortyGigE1/1/1] oam remote-loopback start
```

Related commands

- **oam enable**
- **oam mode**
- **oam remote-loopback interface**

oam remote-loopback interface

Use **oam remote-loopback start interface** to enable Ethernet OAM remote loopback on an Ethernet port.

Use **oam remote-loopback stop interface** to disable Ethernet OAM remote loopback on an Ethernet port.

Syntax

oam remote-loopback start interface *interface-type interface-number*

oam remote-loopback stop interface *interface-type interface-number*

Default

Ethernet OAM remote loopback is disabled on an Ethernet port.

Views

User view, system view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies a port by its type and number.

Usage guidelines

Ethernet OAM remote loopback is available only after the Ethernet OAM connection is established and can be performed only by the Ethernet OAM entities operating in active Ethernet OAM mode.

You can enable Ethernet OAM remote loopback on a specified port in user view or system view, or enable it on the current port in port view. The configurations have the same effect.

Examples

Configure the active Ethernet OAM mode and enable Ethernet OAM on FortyGigE 1/1/1, and then enable Ethernet OAM remote loopback on FortyGigE 1/1/1 in system view.

```
<Sysname> system-view
[Sysname] interface fortygige 1/1/1
[Sysname-FortyGigE1/1/1] oam mode active
[Sysname-FortyGigE1/1/1] oam enable
[Sysname-FortyGigE1/1/1] quit
[Sysname] oam remote-loopback start interface fortygige 1/1/1
```

Related commands

- **oam enable**
- **oam mode**
- **oam remote-loopback**

oam remote-loopback reject-request

Use **oam remote-loopback reject-request** to configure a port to reject the Ethernet OAM remote loopback request from a remote port.

Use **undo oam remote-loopback reject-request** to restore the default.

Syntax

oam remote-loopback reject-request

undo oam remote-loopback reject-request

Default

A port does not reject the Ethernet OAM remote loopback request from a remote port.

Views

Layer 2 Ethernet port view, Layer 3 Ethernet port view

Predefined user roles

network-admin

Usage guidelines

If a port is in loopback state when you execute the **oam remote-loopback reject-request** command, the configuration takes effect when the next loopback starts.

Examples

Configure FortyGigE 1/1/1 to reject the Ethernet OAM remote loopback request from a remote port.

```
<Sysname> system-view
[Sysname] interface fortygige 1/1/1
[Sysname-FortyGigE1/1/1] oam remote-loopback reject-request
```

oam timer hello

Use **oam timer hello** to configure the Ethernet OAM handshake packet transmission interval.

Use **undo oam timer hello** to restore the default.

Syntax

oam timer hello *interval*
undo oam timer hello

Default

The port uses the global setting.

Views

Layer 2 Ethernet port view, Layer 3 Ethernet port view

Predefined user roles

network-admin

Parameters

interval: Specifies the Ethernet OAM handshake packet transmission interval, in steps of 100 (in milliseconds). The value range for this argument is 500 to 5000.

Usage guidelines

After the timeout timer of an Ethernet OAM connection expires, the local OAM entity ages out its connection with the peer OAM entity, causing the OAM connection to disconnect. To keep the Ethernet OAM connections stable, HP recommends that you set the connection timeout timer to be at least five times the handshake packet transmission interval.

The configuration in port view takes effect on the specified port. For a port, the configuration in port view takes precedence.

Examples

```
# Set the Ethernet OAM handshake packet transmission interval to 600 milliseconds.  
<Sysname> system-view  
[Sysname] interface fortygige 1/1/1  
[Sysname-FortyGigE1/1/1] oam timer hello 600
```

Related commands

- **display oam configuration**
- **oam global timer hello**

oam timer keepalive

Use **oam timer keepalive** to configure the Ethernet OAM connection timeout timer.

Use **undo oam timer keepalive** to restore the default.

Syntax

oam timer keepalive *interval*
undo oam timer keepalive

Default

The port uses the global setting.

Views

Layer 2 Ethernet port view, Layer 3 Ethernet port view

Predefined user roles

network-admin

Parameters

interval: Specifies the Ethernet OAM connection timeout timer, in steps of 100 (in milliseconds). The value range for this argument is 1000 to 25000.

Usage guidelines

After the timeout timer of an Ethernet OAM connection expires, the local OAM entity ages out its connection with the peer OAM entity, causing the OAM connection to disconnect. To keep the Ethernet OAM connections stable, HP recommends that you set the connection timeout timer to be at least five times the handshake packet transmission interval.

The configuration in port view takes effect on the specified port. For a port, the configuration in port view takes precedence.

Examples

```
# Set the Ethernet OAM connection timeout timer to 6000 milliseconds.
```

```
<Sysname> system-view  
[Sysname] interface fortygige 1/1/1  
[Sysname-FortyGigE1/1/1] oam timer keepalive 6000
```

Related commands

- **display oam configuration**
- **oam global timer keepalive**

reset oam

Use **reset oam** to clear the statistics of Ethernet OAM packets and Ethernet OAM link error events for an Ethernet port.

Syntax

```
reset oam [ interface interface-type interface-number ]
```

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

Usage guidelines

If you do not specify the **interface** keyword, the command clears the statistics of Ethernet OAM packets and Ethernet OAM link error events for all the ports.

Examples

```
# Clear the statistics of Ethernet OAM packets and Ethernet OAM link error events for all the ports.
```

<Sysname> reset oam

Related commands

- **display oam**
- **display oam link-event**

CFD commands

cfid ais enable

Use **cfid ais enable** to enable AIS.

Use **undo cfid ais enable** to disable AIS.

Syntax

cfid ais enable

undo cfid ais enable

Default

AIS is disabled.

Views

System view

Predefined user roles

network-admin

Examples

```
# Enable AIS.  
<Sysname> system-view  
[Sysname] cfid ais enable
```

Related commands

- **cfid ais level**
- **cfid ais period**

cfid ais level

Use **cfid ais level** to configure the AIS frame transmission level.

Use **undo cfid ais level** to restore the default.

Syntax

cfid ais level *level-value* **service-instance** *instance-id*

undo cfid ais level *level-value* **service-instance** *instance-id*

Default

The AIS frame transmission level is not configured.

Views

System view

Predefined user roles

network-admin

Parameters

level *level-value*: Specifies the AIS frame transmission level in the range of 1 to 7.

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767.

Usage guidelines

If no AIS frame transmission level is configured for a service instance, the MEPs in the service instance cannot send AIS frames.

Examples

```
# Configure the AIS frame transmission level as 3 in service instance 1.
<Sysname> system-view
[Sysname] cfd ais level 3 service-instance 1
```

Related commands

- **cfd ais enable**
- **cfd ais period**

cfd ais period

Use **cfd ais period** to configure the AIS frame transmission period.

Use **undo cfd ais period** to restore the default.

Syntax

cfd ais period *period-value* **service-instance** *instance-id*

undo cfd ais period *period-value* **service-instance** *instance-id*

Default

The AIS frame transmission period is 1 second.

Views

System view

Predefined user roles

network-admin

Parameters

period *period-value*: Specifies the AIS frame transmission period in the range of 1 to 60 seconds.

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767.

Examples

```
# Configure the AIS frame transmission period as 60 seconds in service instance 1.
<Sysname> system-view
[Sysname] cfd ais period 60 service-instance 1
```

Related commands

- **cfd ais enable**
- **cfd ais level**

cfid ais-track link-status global

Use **cfid ais-track link-status global** to enable port status-AIS collaboration.

Use **undo cfid ais-track link-status global** to disable port status-AIS collaboration.

Syntax

cfid ais-track link-status global

undo cfid ais-track link-status global

Default

Port status-AIS collaboration is disabled.

Views

System view

Predefined user roles

network-admin

Examples

```
# Enable port status-AIS collaboration.  
<Sysname> system-view  
[Sysname] cfid ais-track link-status global
```

Related commands

- **cfid ais-track link-status level**
- **cfid ais-track link-status period**
- **cfid ais-track link-status vlan**

cfid ais-track link-status level

Use **cfid ais-track link-status level** to configure the EAIS frame transmission level.

Use **undo cfid ais-track link-status level** to restore the default.

Syntax

cfid ais-track link-status level *level-value*

undo cfid ais-track link-status level

Default

The EAIS frame transmission level is not configured.

Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

level *level-value*: Specifies the EAIS frame transmission level in the range of 0 to 7.

Usage guidelines

If no EAIS frame transmission level is configured on a port, the port cannot send EAIS frames.

Follow these guidelines when you use this command:

- Configurations in Ethernet interface view take effect only on the current interface.
- Configurations in aggregate interface view take effect on the aggregate interface and all its member ports.
- Configurations on a member port take effect only when the member port leaves the aggregation group.

Examples

```
# Configure the EAIS frame transmission level as 3 on FortyGigE 1/1/1.
```

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

```
[Sysname] interface fortygige 1/1/1
```

```
[Sysname-FortyGigE1/1/1] cfd ais-track link-status level 3
```

Related commands

- **cfd ais-track link-status global**
- **cfd ais-track link-status period**
- **cfd ais-track link-status vlan**

cfd ais-track link-status period

Use **cfd ais-track link-status period** to configure the EAIS frame transmission period.

Use **undo cfd ais-track link-status period** to restore the default.

Syntax

```
cfd ais-track link-status period period-value
```

```
undo cfd ais-track link-status period
```

Default

The EAIS frame transmission period is not configured.

Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

period *period-value*: Specifies the EAIS frame transmission period in the range of 1 to 60 seconds.

Usage guidelines

If no EAIS frame transmission period is configured on a port, the port cannot send EAIS frames.

Follow these guidelines when you use this command:

- Configurations in Ethernet interface view take effect only on the current interface.
- Configurations in aggregate interface view take effect on the aggregate interface and all its member ports.

- Configurations on a member port take effect only when the member port leaves the aggregation group.

Examples

```
# Configure the EAIS frame transmission period as 60 seconds on FortyGigE 1/1/1.
<Sysname> system-view
[Sysname] interface fortygige 1/1/1
[Sysname-FortyGigE1/1/1] cfd ais-track link-status period 60
```

Related commands

- **cfd ais-track link-status global**
- **cfd ais-track link-status level**
- **cfd ais-track link-status vlan**

cfd ais-track link-status vlan

Use **cfd ais-track link-status vlan** to specify the VLANs where the EAIS frames can be transmitted.

Use **undo cfd ais-track link-status vlan** to remove the specified VLANs.

Syntax

```
cfd ais-track link-status vlan vlan-list
undo cfd ais-track link-status vlan vlan-list
```

Default

The EAIS frames can be transmitted only within the default VLAN of the port.

Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

vlan *vlan-list*: Specifies the VLANs where the EAIS frames can be transmitted. The *vlan-list* argument specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN ID or a range of VLAN IDs in the form of *vlan-id* [**to** *vlan-id*]. The value range for VLAN IDs is 1 to 4094.

Usage guidelines

The EAIS frames are transmitted within the intersection of the VLANs specified with this command and the existing VLANs on the device.

If the command is executed multiple times, the combination of the VLANs specified in each command takes effect.

Follow these guidelines when you use this command:

- Configurations in Ethernet interface view take effect only on the current interface.
- Configurations in aggregate interface view take effect on the aggregate interface and all its member ports.
- Configurations on a member port take effect only when the member port leaves the aggregation group.

Examples

On port FortyGigE 1/1/1, specify VLANs 100 through 200 as the VLANs where the EAIS frames can be transmitted.

```
<Sysname> system-view
[Sysname] interface fortygige 1/1/1
[Sysname-FortyGigE1/1/1] cfd ais-track link-status vlan 100 to 200
```

Related commands

- **cfd ais-track link-status global**
- **cfd ais-track link-status level**
- **cfd ais-track link-status period**

cfd cc enable

Use **cfd cc enable** to enable CCM sending on a specified MEP.

Use **undo cfd cc enable** to disable CCM sending on a specified MEP.

Syntax

cfd cc service-instance *instance-id* **mep** *mep-id* **enable**

undo cfd cc service-instance *instance-id* **mep** *mep-id* **enable**

Default

The CCM sending function is disabled.

Views

Layer 2/Layer 3 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

service-instance *instance-id*: Specifies the service instance ID in the range of 1 to 32767.

mep *mep-id*: Specifies the ID of a MEP in the range of 1 to 8191.

Usage guidelines

Follow these guidelines when you use this command:

- Configurations in Ethernet interface view take effect only on the current interface.
- Configurations in aggregate interface view take effect on the aggregate interface and all its member ports.
- Configurations on a member port take effect only when the member port leaves the aggregation group.

Examples

On port FortyGigE 1/1/1, enable CCM sending on MEP 3 in service instance 5.

```
<Sysname> system-view
[Sysname] interface fortygige 1/1/1
[Sysname-FortyGigE1/1/1] cfd cc service-instance 5 mep 3 enable
```

Related commands

cfd cc interval

cfd cc interval

Use **cfd cc interval** to set the value of the interval field in the CCM messages.

Use **undo cfd cc interval** to restore default.

Syntax

cfd cc interval *interval-value* **service-instance** *instance-id*

undo cfd cc interval [*interval-value*] **service-instance** *instance-id*

Default

The value of this field is 4 for all CCMs sent.

Views

System view

Predefined user roles

network-admin

Parameters

interval *interval-value*: Specifies the value of the interval field in CCM messages, in the range of 1 to 7.

service-instance *instance-id*: Specifies the service instance ID in the range of 1 to 32767.

Usage guidelines

When setting the CCM interval, use the settings described in [Table 6](#).

Table 6 CCM interval field encoding

| CCM interval field | Transmission interval | Maximum CCM lifetime |
|--------------------|-----------------------|----------------------|
| 1 | 10/3 milliseconds | 35/3 milliseconds |
| 2 | 10 milliseconds | 35 milliseconds |
| 3 | 100 milliseconds | 350 milliseconds |
| 4 | 1 second | 3.5 seconds |
| 5 | 10 seconds | 35 seconds |
| 6 | 60 seconds | 210 seconds |
| 7 | 600 seconds | 2100 seconds |

Examples

```
# Set the value of the interval field in CCMs sent by MEPs in service instance 2 to 7.
```

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

```
[Sysname] cfd cc interval 7 service-instance 2
```

Related commands

cfd cc enable

cfm dm one-way

Use **cfm dm one-way** to enable one-way delay measurement (DM). The one-way DM function measures the one-way frame delay between the source and target MEPs by using 1DM frames.

Syntax

```
cfm dm one-way service-instance instance-id mep mep-id { target-mac mac-address | target-mep target-mep-id } [ number number ]
```

Views

Any view

Predefined user roles

network-admin

Parameters

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767.

mep *mep-id*: Specifies the source MEP by its ID in the range of 1 to 8191.

target-mac *mac-address*: Specifies the target MEP by its MAC address in the format of H-H-H.

target-mep *target-mep-id*: Specifies the target MEP by its ID in the range of 1 to 8191.

number *number*: Specifies the number of 1DM frames sent. The value range for the *number* argument is 2 to 10, and the default is 5.

Usage guidelines

To view the one-way delay test result, use the **display cfm dm one-way history** command on the target MEP.

Examples

```
# Enable the one-way DM function to test the one-way frame delay from source MEP 1101 to target MEP 1003 in service instance 1.
```

```
<Sysname> cfm dm one-way service-instance 1 mep 1101 target-mep 1003  
5 1DMs have been sent. Please check the result on the remote device.
```

Related commands

- **display cfm dm one-way history**
- **reset cfm dm one-way history**

cfm dm two-way

Use **cfm dm two-way** to enable two-way DM. The two-way DM function measures the two-way frame delay between the source and target MEPs by using DMM frames and DMR frames.

Syntax

```
cfm dm two-way service-instance instance-id mep mep-id { target-mac mac-address | target-mep target-mep-id } [ number number ]
```

Views

Any view

Predefined user roles

network-admin

Parameters

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767.

mep *mep-id*: Specifies the source MEP by its ID in the range of 1 to 8191.

target-mac *mac-address*: Specifies the target MEP by its MAC address, which is in the format of H-H-H.

target-mep *target-mep-id*: Specifies the target MEP by its ID in the range of 1 to 8191.

number *number*: Specifies the number of DMM frames sent. The value range for the *number* argument is 2 to 10, and the default is 5.

Examples

```
# Enable the two-way DM function to test the two-way frame delay between source MEP 1101 and target MEP 2001 in service instance 1.
```

```
<Sysname> cfd dm two-way service-instance 1 mep 1101 target-mep 2001
```

```
Frame delay:
```

```
Reply from 0010-fc00-6512: 10ms
```

```
Reply from 0010-fc00-6512: 9ms
```

```
Reply from 0010-fc00-6512: 11ms
```

```
Reply from 0010-fc00-6512: 5ms
```

```
Reply from 0010-fc00-6512: 5ms
```

```
Average: 8ms
```

```
Sent DMMs: 5          Received: 5          Lost: 0
```

```
Frame delay variation: 5ms 4ms 6ms 0ms 0ms
```

```
Average: 3ms
```

Table 7 Command output

| Field | Description |
|---------------------------|--|
| Reply from 0010-fc00-6512 | Delay of the DMR frames returned from the MEP with MAC address 0010-FC00-6512. |
| Average | Average frame delay or average frame delay variation. |
| Sent DMMs | Number of sent DMM frames . |
| Received | Number of received DMR frames. |
| Lost | Number of lost DMM frames. |

cfd enable

Use **cfd enable** to enable CFD.

Use **undo cfd enable** to disable CFD.

Syntax

cfd enable

undo cfd enable

Default

CFD is disabled.

Views

System view

Predefined user roles

network-admin

Examples

```
# Enable CFD.
<Sysname> system-view
[Sysname] cfd enable
```

cfld linktrace

Use **cfld linktrace** to find the path between the source MEP and target MP, which is achieved through the transmission of LTMs between the two and detection of the responding LTRs.

Syntax

```
cfld linktrace service-instance instance-id mep mep-id { target-mac mac-address | target-mep target-mep-id } [ tll tll-value ] [ hw-only ]
```

Views

Any view

Predefined user roles

network-admin

Parameters

service-instance *instance-id*: Specifies the service instance ID in the range of 1 to 32767.

mep *mep-id*: Specifies the ID of the source MEP, in the range of 1 to 8191.

target-mac *mac-address*: Specifies the destination MAC address, in the format of H-H-H.

target-map *target-mep-id*: Specifies the ID of the destination MEP, in the range of 1 to 8191.

tll *tll-value*: Specifies the time to live value in the range of 1 to 255 and defaulting to 64.

hw-only: Sets the hw-only bits of the LTMs sent. If this keyword is specified, the MIP does not flood LTM messages that have an unknown destination MAC address.

Examples

```
# Identify the path between source MEP 1101 and target MEP 2001 in service instance 1.
```

```
<Sysname> cfd linktrace service-instance 1 mep 1101 target-mep 2001
```

```
Linktrace to MEP 2001 with the sequence number 1101-43361:
```

| MAC address | TTL | Last MAC | Relay action |
|----------------|-----|----------------|--------------|
| 0010-fc00-6512 | 63 | 0010-fc00-6500 | Hit |

Table 8 Command output

| Field | Description |
|---|--|
| Linktrace to MEP 2001 with the sequence number 1101-43361 | Linktrace to target MEP 2001 with the sequence number 1101-43361. |
| MAC address | Source MAC address in the LTR messages. |
| TTL | TTL value when the LTM passes the device. |
| Last MAC | MAC address of the last-hop device the LTM passes. |
| Relay action | Indicates whether the forwarding device found the destination MAC address in its MAC address table. When the standard version (IEEE 802.1ag) of CFD is used: <ul style="list-style-type: none">• Hit—The current device is the destination device.• FDB—The forwarding device found the destination MAC address.• MPDB—The destination MAC address is not found, or the destination MAC address is found in the MEP or MIP database. |

Related commands

- **cf** linktrace auto-detection
- **display** cfd linktrace-reply

cfd linktrace auto-detection

Use **cf** linktrace auto-detection to enable the auto sending of linktrace messages.

Use **undo** cfd linktrace auto-detection to disable this function.

Syntax

cf linktrace auto-detection [size *size-value*]

undo cfd linktrace auto-detection

Default

This function is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

size *size-value*: Specifies the size of the buffer used to store the auto-detection result, in the range of 1 to 100 (in terms of sending times).

This value defaults to 5, which means the buffer stores the results of the recent five auto-detections.

Usage guidelines

After LT messages automatic sending is enabled, if the source MEP fails to receive the CCMs from the target MEP within 3.5 times the sending interval, the link between the two is regarded as faulty and LTM messages will be sent out. (The destination of the LTM messages is the target MEP, and the TTL field value is 255.) Based on the LTRs that echo back, the fault source can be located.

Once you disable LT message automatic sending, the content stored in the buffer will be removed.

Examples

```
# Enable automatic LT messages sending, and set the size of the buffer used to store the auto-detection result to 100 (in terms of sending times).
```

```
<Sysname> system-view
[Sysname] cfd linktrace auto-detection size 100
```

Related commands

- **cfd linktrace**
- **display cfd linktrace-reply auto-detection**

cfd loopback

Use **cfd loopback** to enable LB function so that LBMs can be sent from the source MEP to the target MP, and LBR messages can be received.

Syntax

```
cfd loopback service-instance instance-id mep mep-id { target-mac mac-address | target-mep target-mep-id } [ number number ]
```

Views

Any view

Predefined user roles

network-admin

Parameters

service-instance *instance-id*: Specifies the service instance ID in the range of 1 to 32767.

mep *mep-id*: Specifies the ID of the source MEP, in the range of 1 to 8191.

target-mac *mac-address*: Specifies the destination MAC address of the MP, in the format of H-H-H.

target-mep *target-mep-id*: Specifies the ID of the target MEP, in the range of 1 to 8191.

number *number*: Specifies the number of the LBMs packets sent, in the range of 1 to 10. The default is 5.

Examples

```
# Enable LB to check the status of the link between MEP 1101 and MEP 2001 in service instance 1 (assume that the link status is normal).
```

```
<Sysname> cfd loopback service-instance 1 mep 1101 target-mep 2001
Loopback to 0010-fc00-6512 with the sequence number start from 1101-43404:
Reply from 0010-fc00-6512: sequence number=1101-43404 Time=5ms
Reply from 0010-fc00-6512: sequence number=1101-43405 Time=5ms
Reply from 0010-fc00-6512: sequence number=1101-43406 Time=5ms
Reply from 0010-fc00-6512: sequence number=1101-43407 Time=5ms
Reply from 0010-fc00-6512: sequence number=1101-43408 Time=5ms
Sent: 5          Received: 5          Lost: 0
```

```
# Enable LB to check the status of the link between MEP 1101 and MEP 2001 in service instance 1 (assume that the link status is abnormal).
```

```
<Sysname> cfd loopback service-instance 1 mep 1101 target-mep 2001
Loopback to 0010-fc00-6512 with the sequence number start from 1101-43404:
```

Sent: 5 Received: 0 Lost: 5

Table 9 Command output

| Field | Description |
|---|---|
| Loopback to 0010-fc00-6512 with the sequence number start from 1101-43404 | Sends LBMs to 0010-FC00-6512 with the sequence number starting with 1101-43404. |
| Reply from 0010-fc00-6512 | Reply from the MP with the MAC address 0010-FC00-6512. |
| sequence number | Sequence number in the LBR messages. |
| Time=5ms | The interval between the sending of LBMs and receiving of LBRs is 5 milliseconds. |
| Sent | Number of LBMs sent. |
| Received | Number of LBR messages received. |
| Lost | Number of lost LBRs. |

cfm md

Use **cfm md** to create an MD.

Use **undo cfm md** to delete an MD.

Syntax

```
cfm md md-name [ index index-value ] level level-value [ md-id { dns dns-name | mac mac-address subnumber | none } ]
```

```
undo cfm md md-name
```

Default

No MD is created.

Views

System view

Predefined user roles

network-admin

Parameters

md *md-name*: Specifies the name of an MD, which is a string of 1 to 43 characters that can contain letters, numbers, and special characters such as grave accent (`), tilde (~), exclamation mark (!), at sign (@), number sign (#), dollar sign (\$), percent (%), caret (^), ampersand (&), asterisk(*), brackets { }, (), [], < >, hyphen (-), underscore (_), plus (+), equal sign (=), vertical bar (|), colon (:), semicolon (;), quotation mark ("), comma (,), period (.), and slash (/).

index *index-value*: Specifies an MD index in the range of 1 to 4294967295. If this option is not specified, the system automatically assigns the smallest index number that is not in use. HP recommends that you use the index automatically assigned by the system.

level *level-value*: Specifies an MD level in the range of 0 to 7.

md-id: Specifies the MD name carried by packets sent by the MEP. If you do not provide the keyword, the MD name is represented by *md-name*.

dns *dns-name*: Specifies an MD name in the format of DNS name, where *dns-name* represents the DNS name.

mac *mac-address subnumber*: Specifies an MD name comprising the MAC address and an integer, where *mac-address* represents the MAC address of the MD, and *subnumber* is in the range of 0 to 65535.

none: Configures the packets sent by the MEP to not carry any MD name.

Usage guidelines

An MD name must be in compliant with the specifications in table 21-19 in IEEE802.1ag-2007.

You can create only one MD with a specific level. MD cannot be created if you enter an invalid MD name or an existing MD name or the MD index is in use.

When deleting an MD, you will also delete the configurations related to that MD.

Examples

Create an MD named **test_md1**, with its level being 3.

```
<Sysname> system-view
[Sysname] cfd md test_md1 level 3
```

Create an MD named **test_md2**, and the MD name carried in the packet sent by the MEP comprises the MAC address 1-1-1 and integer 1.

```
<Sysname> system-view
[Sysname] cfd md test_md2 level 5 md-id mac 1-1-1 1
```

cfd mep

Use **cfd mep** to create a MEP.

Use **undo cfd mep** to delete the specified MEP.

Syntax

Layer 2 Ethernet interface view or Layer 2 aggregate interface view:

```
cfd mep mep-id service-instance instance-id { inbound | outbound }
```

```
undo cfd mep mep-id service-instance instance-id
```

Layer 3 Ethernet interface view:

```
cfd mep mep-id service-instance instance-id outbound
```

```
undo cfd mep mep-id service-instance instance-id
```

Default

No MEP exists on a port.

Views

Layer 2/Layer 3 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

mep-id: Specifies the ID of a MEP, in the range of 1 to 8191.

service-instance *instance-id*: Specifies the service instance ID in the range of 1 to 32767.

inbound: Creates an inward-facing MEP.

outbound: Creates an outward-facing MEP.

Usage guidelines

In creating a MEP, the service instance you specified defines the MD and MA to which the MEP belongs.

You cannot create a MEP if the MEP ID is not included in the MEP list of the relevant service instance.

Follow these guidelines when you use this command:

- Configurations in Ethernet interface view take effect only on the current interface.
- Configurations in aggregate interface view take effect on the aggregate interface and all its member ports.
- Configurations on a member port take effect only when the member port leaves the aggregation group.

Examples

```
# Configure a MEP list in service instance 5, and create inward-facing MEP 3 in service instance 5 on
FortyGigE 1/1/1.
```

```
<Sysname> system-view
[Sysname] cfd md test_md level 3
[Sysname] cfd service-instance 5 ma-id vlan-based md test_md vlan 100
[Sysname] cfd meplist 3 service-instance 5
[Sysname] interface fortygige 1/1/1
[Sysname-FortyGigE1/1/1] cfd mep 3 service-instance 5 outbound
```

Related commands

cfd meplist

cfd meplist

Use **cfd meplist** to create a MEP list, a collection of local MEPs allowed to be configured and the remote MEPs to be monitored in the same MA.

Use **undo cfd meplist** to delete existing MEP lists.

Syntax

cfd meplist *mep-list* **service-instance** *instance-id*

undo cfd meplist *mep-list* **service-instance** *instance-id*

Default

No MEP list is created.

Views

System view

Predefined user roles

network-admin

Parameters

mep-list *mep-list*: Specifies a list of up to 10 MEP IDs or MEP ID ranges in the format of *mep-list* = { *mep-id* [to *mep-id*] }&<1-10>. The *mep-id* argument represents the MEP ID and is in the range of 1 to 8191.

service-instance *instance-id*: Specifies the service instance ID in the range of 1 to 32767.

Usage guidelines

Before creating a MEP list, create the relevant MD, MA, and service instance.

After you delete a MEP list, all local MEP configurations based on this list are deleted.

Examples

```
# Create a MEP list that includes MEP 9 through MEP 15 in service instance 5.
```

```
<Sysname> system-view
[Sysname] cfd md test_md level 3
[Sysname] cfd service-instance 5 ma-id vlan-based md test_md vlan 100
[Sysname] cfd meplist 9 to 15 service-instance 5
```

Related commands

- **cfd md**
- **cfd service-instance**

cfd mip-rule

Use **cfd mip-rule** to configure the rules for generating MIPs. The system automatically generates MIPs on each port according to the rules configured.

Use **undo cfd mip-rule** to restore the default.

Syntax

```
cfd mip-rule { default | explicit } service-instance instance-id
```

```
undo cfd mip-rule [ default | explicit ] service-instance instance-id
```

Default

No rules for generating MIPs are configured and the system does not automatically generate any MIPs.

Views

System view

Predefined user roles

network-admin

Parameters

default: Specifies the default rule. If no lower-level MIP exists on an interface, a MIP is created on the current level. A MIP can be created even if no MEP is configured on the interface.

explicit: Specifies the explicit rule. If no lower-level MIP exists and a lower-level MEP exists on an interface, a MIP is created at the current level. A MIP can be created only when a lower-level MEP is created on the interface.

service-instance *instance-id*: Specifies the service instance ID in the range of 1 to 32767.

Examples

```
# Configure the MIP generation rule as default in service instance 5.
```

```
<Sysname> system-view
[Sysname] cfd mip-rule default service-instance 5
```

cfid service-instance

Use **cfid service-instance** to create a service instance with the MD name.

Use **undo cfd service-instance** to remove the service instance.

Syntax

```
cfid service-instance instance-id ma-id { icc-based ma-name | integer ma-num | string ma-name | vlan-based [ vlan-id ] } [ ma-index index-value ] md md-name [ vlan vlan-id ]
```

```
undo cfd service-instance instance-id
```

Default

No service instance exists.

Views

System view

Predefined user roles

network-admin

Parameters

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767.

ma-id: Creates an MA.

icc-based *ma-name*: Configures an MA to be identified by an ICC. The *ma-name* argument is a string of 1 to 13 characters.

integer *ma-num*: Configures an MA to be identified by an integer, where the *ma-num* argument is in the range of 0 to 65535.

string *ma-name*: Configures an MA to be identified by a string, where the *ma-name* argument is string of 1 to 45 characters that can contain letters, numbers, and special characters such as *grave accent* (`), tilde (~), exclamation mark (!), at sign (@), number sign (#), dollar sign (\$), percent (%), caret (^), ampersand (&), asterisk(*), brackets ({ }, (), [], < >), hyphen (-), underscore (_), plus (+), equal sign (=), vertical bar (|), colon (:), semicolon (;), quotation mark ('), comma (,), period (.), and slash (/).

vlan-based [*vlan-id*]: Configures an MA to be identified by a VLAN ID, where the *vlan-id* argument is in the range of 1 to 4094. If you do not provide the *vlan-id* argument, the VLAN ID specified by **vlan** *vlan-id* is used. If the **vlan** *vlan-id* option is not provided, you must specify the *vlan-id* argument for the **vlan-based** [*vlan-id*] option.

ma-index *index-value*: Specifies an MA index in the range of 1 to 4294967295. If this option is not specified, the system automatically assigns the smallest index number that is not in use. HP recommends that you use the index automatically assigned by the system.

md *md-name*: Specifies the name of an MD. The *md-name* argument is a string of 1 to 43 characters that can contain letters, numbers, and special characters such as *grave accent* (`), tilde (~), exclamation mark (!), at sign (@), number sign (#), dollar sign (\$), percent (%), caret (^), ampersand (&), asterisk(*), brackets ({ }, (), [], < >), hyphen (-), underscore (_), plus (+), equal sign (=), vertical bar (|), colon (:), semicolon (;), quotation mark ('), comma (,), period (.), and slash (/).

vlan *vlan-id*: Specifies the VLAN that the MA serves, in the range of 1 to 4094.

Usage guidelines

A service instance is indicated by an integer to represent an MA in an MD. The MD and MA define the level attribute and VLAN attribute of the messages handled by the MPs in a service instance. An MA index uniquely identifies a specific MA in an MD. An MA index can be used in different MDs.

An MD name must be in compliant with the specifications in table 21-19 in IEEE802.1ag-2007.

With the **vlan-based** [*vlan-id*] or **vlan** *vlan-id* option, the command creates an MA carrying the VLAN attribute. If you do not specify the option, the command creates an MA carrying no VLAN attribute.

You must create the relevant MD and MA prior to creating a service instance with the MD name.

When you delete a service instance, you are deleting the configurations related to that service instance as well.

Deleting a service instance not only breaks up the connection between the service instance and the relevant MA, but also deletes the MA itself.

Examples

```
# Create a level-3 MD named test_md and create service instance 5, in which the MA is identified by a VLAN and serves VLAN 100.
```

```
<Sysname> system-view
[Sysname] cfd md test_md level 3
[Sysname] cfd service-instance 5 ma-id vlan-based md test_md vlan 100
```

Related commands

cfd md

cfd slm

Use **cfd slm** to enable loss measurement (LM). The LM function measures the frame loss between the source and target MEPs by using LMM frames and LMR frames.

Syntax

```
cfd slm service-instance instance-id mep mep-id { target-mac mac-address | target-mep target-mep-id }
[ number number ]
```

Views

Any view

Predefined user roles

network-admin

Parameters

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767.

mep *mep-id*: Specifies the source MEP by its ID in the range of 1 to 8191.

target-mac *mac-address*: Specifies the target MEP by its MAC address, which is in the format of H-H-H.

target-mep *target-mep-id*: Specifies the target MEP by its ID in the range of 1 to 8191.

number *number*: Specifies the number of LMM frames sent. The value range for the *number* argument is 2 to 10, and the default is 5.

Examples

```
# Enable the LM function to measure the frame loss between source MEP 1101 and target MEP 2001 in service instance 1.
```

```
<Sysname> cfd slm service-instance 1 mep 1101 target-mep 2001
Reply from 0010-fc00-6512
Far-end frame loss: 10    Near-end frame loss: 20
Reply from 0010-fc00-6512
Far-end frame loss: 40    Near-end frame loss: 40
Reply from 0010-fc00-6512
Far-end frame loss: 0     Near-end frame loss: 10
Reply from 0010-fc00-6512
Far-end frame loss: 30    Near-end frame loss: 30

Average
Far-end frame loss: 20    Near-end frame loss: 25
Far-end frame loss rate: 25.00%    Near-end frame loss rate: 32.00%
Sent LMMs: 5    Received: 5    Lost: 0
```

Table 10 Command output

| Field | Description |
|---------------------------|--|
| Reply from 0010-fc00-6512 | LMR frames returned from the target MEP with MAC address 0010-FC00-6512. |
| Far-end frame loss | Number of lost frames on the target MEP. |
| Near-end frame loss | Number of lost frames on the source MEP. |
| Far-end frame loss rate | Frame loss ratio on the target MEP. |
| Near-end frame loss rate | Frame loss ratio on the source MEP. |
| Average | Average number of lost frames. |
| Sent LMMs | Number of sent LMM frames. |
| Received | Number of received LMR frames. |
| Lost | Number of lost LMR frames. |

cfd tst

Use **cfd tst** to enable test (TST). The TST function detects bit errors between the source and target MEPs by using TST frames.

Syntax

```
cfd tst service-instance instance-id mep mep-id { target-mac mac-address | target-mep target-mep-id }
[ number number ] [ length-of-test length ] [ pattern-of-test { all-zero | prbs } [ with-crc ] ]
```

Views

Any view

Predefined user roles

network-admin

Parameters

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767.

mep *mep-id*: Specifies the source MEP by its ID in the range of 1 to 8191.

target-mac *mac-address*: Specifies the target MEP by its MAC address, which is in the format of H-H-H.

target-mep *target-mep-id*: Specifies the target MEP by its ID in the range of 1 to 8191.

number *number*: Specifies the number of sent TST frames. The value range for the *number* argument is 1 to 10, and the default is 5.

length-of-test *length*: Specifies the length of the Test TLV (Type/Length/Value) in the TST frame. The value range for the *length* argument is 4 to 1400, and the default is 64.

pattern-of-test { **all-zero** | **prbs** } [**with-crc**]: Specifies the pattern of the Test TLV in the TST frame:

- **all-zero** (all-zero value without CRC-32), which is the default pattern.
- **prbs** (pseudo random bit sequence without CRC-32).
- **all-zero with-crc** (all-zero value with CRC-32).
- **prbs with-crc** (pseudo random bit sequence with CRC-32).

Usage guidelines

To view the TST test result, use the **display cfd tst** command on the target MEP.

Examples

```
# Enable the TST function to test the bit errors between source MEP 1101 and target MEP 1003 in service instance 1.
```

```
<Sysname> cfd tst service-instance 1 mep 1101 target-mep 1003
```

```
5 TSTs have been sent. Please check the result on the remote device.
```

Related commands

- **display cfd tst**
- **reset cfd tst**

display cfd ais

Use **display cfd ais** to display the AIS configuration and information on the specified MEP.

Syntax

```
display cfd ais [ service-instance instance-id [ mep mep-id ] ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767. If you do not specify this option, the command displays the AIS configuration and information for all service instances.

mep mep-id: Specifies a MEP by its ID in the range of 1 to 8191. If you do not specify this option, the command displays the AIS configuration and information for all MEPs.

Examples

Display the AIS configuration and information for all the MEPs in all service instances.

```
<Sysname> display cfd ais
Service instance: 5
AIS level: 4    AIS period: 1s
MEP ID: 1
AIS condition: yes    Time to enter the condition: 2014/01/22 10:43:57
AIS state machine: Previous state: NO_RECEIVE
                  Current state: RECEIVE

MEP ID: 2
AIS condition: yes    Time to enter the condition: 2014/01/22 10:43:57
AIS state machine: Previous state: NO_RECEIVE
                  Current state: RECEIVE

Service instance: 20
AIS level: 3    AIS period: 60s
MEP ID: 10
AIS condition: yes    Time to enter the condition: 2014/01/22 10:43:57
AIS state machine: Previous state: NO_RECEIVE
                  Current state: RECEIVE

Service instance: 100
AIS level: 6    AIS period: 1s
MEP ID: 20
AIS condition: no    Time to enter the condition: 2014/01/22 11:40:01
AIS state machine: Previous state: IDLE
                  Current state: NO_RECEIVE

MEP ID: 50
AIS condition: no    Time to enter the condition: -
AIS state machine: Previous state: IDLE
                  Current state: NO_RECEIVE
```

Table 11 Command output

| Field | Description |
|-----------------------------|---|
| Service instance | Service instance of the MEP. |
| AIS level | AIS frame transmission level. |
| AIS period | AIS frame transmission period. |
| AIS condition | AIS status: <ul style="list-style-type: none"> yes—AIS is running. no—AIS is not running. |
| Time to enter the condition | Time when the AIS status began. (- means AIS is enabled but the MEP does not receive any AIS frame.) |
| AIS state machine | AIS frame receiving state machine. |

| Field | Description |
|----------------|---|
| Previous state | Previous state: <ul style="list-style-type: none"> • IDLE—Not activated. • NO_RECEIVE—Activated. • RECEIVE—AIS frames are received. |
| Current state | Current state: <ul style="list-style-type: none"> • IDLE—Not activated. • NO_RECEIVE—Activated. • RECEIVE—AIS frames are received. |

display cfd ais-track link-status

Use **display cfd ais-track link-status** to display the configuration and information for the AIS associated with the port status.

Syntax

```
display cfd ais-track link-status [ interface interface-type interface-number ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify this option, this command displays the configuration and information for the AIS associated with the status of all ports.

Examples

```
# Display the configuration and information for the AIS associated with the status of all ports.
```

```
<Sysname> display cfd ais-track link-status
```

```
AIS tracking link-status is enabled.
```

```
Interface FortyGigE1/1/1:
```

```
AIS level: 5           AIS period: 1s
```

```
Configured VLANs: 1, 10-100, 103
```

```
Send VLANs: 1, 10-100, 103
```

```
AIS condition: yes     Time to enter the condition: 2014/02/26 10:43:57
```

```
Interface FortyGigE1/1/2:
```

```
AIS level: 5           AIS period: 1s
```

```
Configured VLANs: 1-4094
```

```
Send VLANs: 1-2000
```

```
AIS condition: yes     Time to enter the condition: 2014/02/26 10:44:57
```

Table 12 Command output

| Field | Description |
|--------------------------------------|--|
| AIS tracking link-status is enabled | Port status-AIS collaboration is enabled. |
| AIS tracking link-status is disabled | Port status-AIS collaboration is disabled. |
| Interface | Port that collaborates with AIS. |
| AIS level | EAIS frame transmission level on the port. |
| AIS period | EAIS frame transmission period on the port. |
| Configured VLANs | VLANs where the EAIS frames can be transmitted. |
| Send VLANs | Actual VLANs where the EAIS frames can be transmitted. |
| AIS condition | EAIS frame sending status: <ul style="list-style-type: none">• yes—EAIS frames are being sent.• no—No EAIS frame is being sent. |
| Time to enter the condition | Time when the EAIS frame sending started. |

display cfd dm one-way history

Use **display cfd dm one-way history** to display the one-way DM result.

Syntax

```
display cfd dm one-way history [ service-instance instance-id [ mep mep-id ] ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767. If you do not specify this option, this command displays the one-way DM results for all service instances.

mep *mep-id*: Specifies a MEP by its ID in the range of 1 to 8191. If you do not specify this option, this command displays the one-way DM results for all MEPs.

Usage guidelines

The one-way DM results for all inward-facing MEPs in a service instance are the same.

Examples

```
# Display the one-way DM results for all the MEPs in all service instances.  
<Sysname> display cfd dm one-way history  
Service instance: 1  
MEP ID: 1003  
Sent 1DM total number: 0  
Received 1DM total number: 5  
Frame delay: 10ms 9ms 11ms 5ms 5ms
```

```

Delay average: 8ms
Frame delay variation: 5ms 4ms 6ms 0ms 0ms
Variation average: 3ms
MEP ID: 1004
Sent 1DM total number: 0
Received 1DM total number: 5
Frame delay: 10ms 9ms 11ms 5ms 5ms
Delay average: 8ms
Delay variation: 5ms 4ms 6ms 0ms 0ms
Variation average: 3ms

```

```

Service instance: 2
No MEP exists in the service instance.

```

```

Service instance: 3
MEP ID: 1023
Sent 1DM total number: 5
Received 1DM total number: 10
Frame delay: 20ms 9ms 8ms 7ms 1ms 5ms 13ms 17ms 9ms 10ms
Delay average: 9ms
Delay variation: 19ms 8ms 7ms 6ms 0ms 4ms 12ms 16ms 8ms 9ms
Variation average: 8ms

```

```

Service instance: 4
MEP ID: 1023
Sent 1DM total number: 77
Received 1DM total number: 0

```

Table 13 Command output

| Field | Description |
|---------------------------|--------------------------------|
| Service instance | Service instance of the MEP. |
| Sent 1DM total number | Number of sent 1DM frames. |
| Received 1DM total number | Number of received 1DM frames. |
| Delay average | Average frame delay. |
| Delay variation | Frame delay variation. |
| Variation average | Average frame delay variation. |

Related commands

- **cfldm one-way**
- **reset cfdm one-way history**

display cfd linktrace-reply

Use **display cfd linktrace-reply** to display the LTR information received by a MEP.

Syntax

```
display cfd linktrace-reply [ service-instance instance-id [ mep mep-id ] ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

service-instance *instance-id*: Specifies the service instance ID in the range of 1 to 32767. If you do not specify this option, the LTR information for all service instances is displayed.

mep *mep-id*: Specifies the ID of a MEP, in the range of 1 to 8191. If you do not specify this option, the LTR information for all MEPs is displayed.

Usage guidelines

This command displays only information about LTRs received by execution of the **cfd linktrace** command.

Examples

Display the LTR information for all the MEPs in every service instance.

```
<Sysname> display cfd linktrace-reply
Service instance: 1      MEP ID: 1003
MAC address            TTL      Last MAC              Relay action
0000-fc00-6505        63      0000-fc00-6504      MPDB
000f-e269-a852        62      0000-fc00-6505      FDB
0000-fc00-6508        61      000f-e269-a852      Hit
Service instance: 2      MEP ID: 1023
MAC address            TTL      Last MAC              Relay action
0000-fc00-6508        61      000f-e269-a852      Hit
```

Table 14 Command output

| Field | Description |
|------------------|--|
| Service instance | Service instance to which the MEPs that send LTRs belong. |
| MEP ID | ID of the MEP that sends LTRs. |
| MAC address | Source MAC address in the LTR message. |
| TTL | TTL value when LTR passes the device. |
| Last MAC | MAC address of the last-hop device the LTR passes. |
| Relay action | Indicates whether the forwarding device found the destination MAC address in its MAC address table. When the standard version (IEEE 802.1ag) of CFD is used: <ul style="list-style-type: none">• Hit—The current device is the destination device.• FDB—The forwarding device found the destination MAC address.• MPDB—The destination MAC address is not found, or the destination MAC address is found in the MEP or MIP database. |

Related commands

cf linktrace

display cfd linktrace-reply auto-detection

Use **display cfd linktrace-reply auto-detection** to display information about the LTR messages received as responses to the automatically sent LTMs.

Syntax

display cfd linktrace-reply auto-detection [**size** *size-value*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

size *size-value*: Specifies the times of recent auto-detections, in the range of 1 to 100. If you do not specify this option, all information in the buffer is displayed.

Usage guidelines

This command displays only information about LTRs received by execution of the **cf** linktrace **auto-detection** command.

Examples

Display the contents of the LTRs received as responses to the LTMs automatically sent.

```
<Sysname> display cfd linktrace-reply auto-detection
Service instance: 1      MEP ID: 1003      Time: 2014/05/22 10:43:57
Target MEP ID: 2005    TTL: 255
MAC address            TTL      Last MAC          Relay action
0000-fc00-6505        254     0000-fc00-6504   MPDB
000f-e269-a852        62      0000-fc00-6505   FDB
0000-fc00-6508        61      000f-e269-a852   Hit
Service instance: 2      MEP ID: 1023      Time: 2014/05/22 10:44:06
Target MEP ID: 2025    TTL: 255
MAC address            TTL      Last MAC          Relay action
0000-fc00-6508        61      000f-e269-a852   Hit
```

Table 15 Command output

| Field | Description |
|------------------|---|
| Service instance | Service instance to which the MEPs that sent LTM messages belong. |
| MEP ID | ID of the MEP that sends LTMs. |
| Time | Time of the LTMs automatically sent. |
| Target MEP ID | ID of the target MEP. |
| TTL | Initial TTL value of the automatically sent LTMs. |

| Field | Description |
|--------------|---|
| MAC address | Source MAC address in the LTR messages. |
| TTL | TTL value when LTM passes the device. |
| Last MAC | MAC address of the last-hop device the LTM passes. |
| Relay action | <p>Indicates whether the forwarding device found the destination MAC address in its MAC address table.</p> <p>When the standard version (IEEE 802.1ag) of CFD is used:</p> <ul style="list-style-type: none"> • Hit—The current device is the destination device. • FDB—The forwarding device found the destination MAC address. • MPDB—The destination MAC address is not found, or the destination MAC address is found in the MEP or MIP database. |

Related commands

cfld linktrace auto-detection

display cfd md

Use **display cfd md** to display the MD configuration information.

Syntax

display cfd md

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the MD configuration information.

```
<Sysname> display cfd md
```

CFD is enabled.

Maintenance domains configured: 4 in total

| Level | Index | Maintenance domain | MD format | MD ID |
|-------|-------|--------------------|------------|------------------|
| 0 | 1 | md_0 | CHARSTRING | md_0 |
| 1 | 2 | md_1 | DNS | dns1 |
| 2 | 3 | md_2 | MAC | 0001-0001-0001-1 |
| 3 | 4 | md_3 | NONE | Without ID |

Table 16 Command output

| Field | Description |
|--------------------------------|---------------------------|
| Maintenance domains configured | Number of MDs configured. |
| Level | Level of MD. |
| Index | MD index. |
| Maintenance domain | Name of MD. |

| Field | Description |
|-----------|---|
| MD format | MD name format: <ul style="list-style-type: none"> • CHARSTRING—Character string. • DNS—DNS name. • MAC—MAC address and an integer. • NONE—No MD name is carried. |
| MD ID | MD ID value: <ul style="list-style-type: none"> • A character string if the MD format is CHARSTRING. • A DNS name if the MD format is DNS. • A MAC address-subnumber if the MD format is MAC. • No ID if the MD format is NONE. |

display cfd mep

Use **display cfd mep** to display the attribute and operating information of a MEP.

Syntax

display cfd mep *mep-id* **service-instance** *instance-id*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

mep *mep-id*: Specifies a MEP by its ID in the range of 1 to 8191.

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767.

Examples

Display the attribute and operating information of MEP 50 in service instance 1.

```
<Sysname> display cfd mep 50 service-instance 1
Interface: FortyGigE1/1/2
Maintenance domain: md_0
Maintenance domain index: 1
Maintenance association: ma_0
Maintenance association index: 1
Level: 0          VLAN: 1          Direction: Outbound
Current state: Active          CCM send: Enable
FNG state: FNG_DEFECT_REPORTED

CCM:
Current state: CCI_WAITING
Interval: 1s          SendCCM: 12018
```

Loopback:
 NextSeqNumber: 8877
 SendLBR: 0 ReceiveInOrderLBR: 0 ReceiveOutOrderLBR: 0

Linktrace:
 NextSeqNumber: 8877
 SendLTR: 0 ReceiveLTM: 0

No CCM received from some remote MEPs.

One or more streams of error CCMs is received. The last received CCM:

Maintenance domain: (Without ID)
 Maintenance association: matest1
 MEP ID: 5 Sequence Number: 0x50A
 MAC Address: 0011-2233-4402
 Received Time: 2014/03/06 13:01:34

One or more streams of cross-connect CCMs is received. The last received CCM:

Maintenance domain: mdtest1
 Maintenance association:matest1
 MEP ID: 6 Sequence Number: 0x63A
 MAC Address: 0011-2233-4401
 Received Time: 2014/03/06 13:01:34

Some other MEPs are transmitting the RDI bit.

Table 17 Command output

| Field | Description |
|-------------------------------|---|
| Interface | Interface to which an MD belongs. |
| Maintenance domain | MD to which a MEP belongs. (If the MD does not have a name, this field is displayed as Without ID.) |
| Maintenance domain index | Index of the MD where the MEP resides. |
| Maintenance association | MA to which a MEP belongs. |
| Maintenance association index | Index of the MA where the MEP resides. |
| Level | Level of the MD. |
| VLAN | VLAN to which the MA belongs. |
| Direction | Direction of the MEPs. |
| Current state | State of MEP, either Active or Inactive. |
| CCM send | Whether the MEP sends CCM. |

| Field | Description |
|--|---|
| FNG state | <p>State of FNG (Fault Notification Generator):</p> <ul style="list-style-type: none"> • FNG_RESET—A fault has been cleared. • FNG_DEFECT—A fault has been detected. • FNG_REPORT_DEFECT—Report a fault. • FNG_DEFECT_REPORTED—A fault has been reported. • FNG_DEFECT_CLEARING—A fault is being cleared. <p>If this field is not supported, a hyphen (-) is displayed.</p> |
| CCM | Information related to CCM. |
| Current state | <p>State of CCMs sent:</p> <ul style="list-style-type: none"> • CCI_IDLE—Initial state. • CCI_WAITING—Sending state. <p>If this field is not supported, a hyphen (-) is displayed.</p> |
| Interval | Interval to send CCM. |
| SendCCM | <p>Number of CCMs that have been sent by the MEPs.</p> <p>If this field is not supported, a hyphen (-) is displayed.</p> |
| Loopback | Information related to Loopback. |
| NextSeqNumber | Sequence number of the next LBM to be sent. |
| SendLBR | Number of LBRs that have been sent. If the MEP is inward-facing, the number of LBRs will not be counted. |
| ReceiveInOrderLBR | Number of LBR messages received in correct sequence. |
| ReceiveOutOrderLBR | Number of LBR messages received out of order. |
| Linktrace | Information related to linktrace. |
| NextSeqNumber | Sequence number of the next LTM to be sent. |
| SendLTR | Number of LTRs sent. If the MEP is inward-facing, the number of LTRs will not be counted. |
| ReceiveLTM | Number of LTMs received. |
| No CCM received from some remote MEPs | Failure to receive CCMs from some remote MEPs. (This information is displayed only when some CCMs are lost.) |
| One or more streams of error CCMs is received. The last received CCM | Display the content of the last error CCM when one or more error CCMs are received. (This information is displayed only when error CCMs are received.) |
| Maintenance domain | <p>MD of the last error CCM message.</p> <p>If this field is not supported, a hyphen (-) is displayed.</p> |
| Maintenance association | <p>MA of the last error CCM message.</p> <p>If this field is not supported, a hyphen (-) is displayed.</p> |
| MEP | <p>ID of the MEP that sent the last error CCM message.</p> <p>If this field is not supported, a hyphen (-) is displayed.</p> |
| Sequence Number | <p>Sequence number of the last error CCM.</p> <p>If this field is not supported, a hyphen (-) is displayed.</p> |

| Field | Description |
|--|---|
| Received Time | Time when the last error CCM is received. If this field is not supported, a hyphen (-) is displayed. |
| One or more streams of cross-connect CCMs is received. The last received CCM | Cross-connect CCMs are received, and the content of the last cross-connect CCM is displayed. (This information is displayed only when cross-connect CCMs are received.) |
| Some other MEPs are transmitting the RDI bit. | CCMs with the RDI flag bits set are received from other MEPs. (This information is displayed only when this type of CCMs are received.) |

display cfd meplist

Use **display cfd meplist** to display the MEP list in a service instance.

Syntax

```
display cfd meplist [ service-instance instance-id ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767. If you do not specify this option, MEP lists in all service instances are displayed.

Examples

```
# Display the MEP list in service instance 5.
<Sysname> display cfd meplist service-instance 5
Service instance: 5
MEP list: 1 to 20, 30, 50.
```

display cfd mp

Use **display cfd mp** to display the MP information.

Syntax

```
display cfd mp [ interface interface-type interface-number ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its port type and port number. If you do not specify this option, MP information on all ports is displayed.

Usage guidelines

The output is arranged by port name. On a port, the output shows MPs that serve VLANs, and then shows MPs that do not serve any VLANs. The MPs that serve VLANs are displayed in the ascending VLAN ID order. Within the same VLAN, the output is in the order of MIPs and MEPs (from high to low level). The MEPs that do not serve any VLANs are displayed by level (from high to low).

Examples

```
# Display the MP information on all ports.
```

```
<Sysname> display cfd mp
```

```
Interface FortyGigE1/1/1   VLAN 100
```

```
MIP           Level: 2   Service instance: 102
```

```
Maintenance domain: md_2
```

```
Maintenance domain index: 3
```

```
Maintenance association: ma_2
```

```
Maintenance association index: 3
```

```
MEP ID: 101   Level: 1   Service instance: 101   Direction: Inbound
```

```
Maintenance domain: md_1
```

```
Maintenance domain index: 2
```

```
Maintenance association: ma_1
```

```
Maintenance association index: 2
```

```
MEP ID: 100   Level: 0   Service instance: 100   Direction: Outbound
```

```
Maintenance domain: md_0
```

```
Maintenance domain index: 1
```

```
Maintenance association: ma_0
```

```
Maintenance association index: 1
```

Table 18 Command output

| Field | Description |
|-----------------------------------|--|
| Interface FortyGigE1/1/1 VLAN 100 | MP configuration of VLAN 100 on the FortyGigE 1/1/1. |
| MIP | A MIP in the MP. |
| Level | MD level to which an MP belongs. |
| Service instance | Service instance to which the MP belongs. |
| Maintenance domain | MD to which an MP belongs. |
| Maintenance domain index | Index of the MD to which an MP belongs. |
| Maintenance association | MA to which an MP belongs. |
| Maintenance association index | Index of the MA to which an MP belongs. |
| Direction | Direction of the MEP, inbound or outbound. |

display cfd remote-mep

Use **display cfd remote-mep** to display information about a remote MEP.

Syntax

display cfd remote-mep service-instance *instance-id* **mep** *mep-id*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767.

mep *mep-id*: Specifies a MEP by its ID in the range of 1 to 8191.

Examples

Display remote MEP information for MEP 10 in service instance 4.

```
<Sysname> display cfd remote-mep service-instance 4 mep 10
```

| MEP ID | MAC address | State | Time | MAC status |
|--------|----------------|--------|---------------------|------------|
| 20 | 00e0-fc00-6565 | OK | 2014/03/06 02:36:38 | UP |
| 30 | 00e0-fc27-6502 | OK | 2014/03/06 02:36:38 | DOWN |
| 40 | 00e0-fc00-6510 | FAILED | 2014/03/06 02:36:39 | DOWN |
| 50 | 00e0-fc52-baa0 | OK | 2014/03/06 02:36:44 | DOWN |
| 60 | 0010-fc00-6502 | OK | 2014/03/06 02:36:42 | DOWN |

Table 19 Command output

| Field | Description |
|-------------|---|
| MEP ID | ID of the remote MED. |
| MAC address | MAC address of the remote MEP device. If this field is not supported, a hyphen (-) is displayed. |
| State | Running state of the remote MEP, OK or FAILED. |
| Time | Time when the remote MEP entered the FAILED or OK state for the last time. If this field is not supported, a hyphen (-) is displayed. |
| MAC status | State of the interface indicated by the last CCM received from the remote MEP: <ul style="list-style-type: none">• UP—The interface is ready to pass packets.• DOWN—The interface cannot pass packets.• TESTING—The interface is in some test mode.• UNKNOWN—The interface status cannot be determined.• DORMANT—The interface is not in a state to pass packets. Instead, it is in a pending state, waiting for some external event.• NOT-PRESENT—Some component of the interface is missing.• LLD—The interface is down due to state of the lower layer interfaces. If this field is not supported, a hyphen (-) is displayed. |

display cfd service-instance

Use **display cfd service-instance** to display the configuration information of service instance.

Syntax

```
display cfd service-instance [ instance-id ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

instance-id: Specifies a service instance ID in the range of 1 to 32767. If you do not specify this argument, the configuration information of all service instances is displayed.

Examples

Display the configuration information of all service instances.

```
<Sysname> display cfd service-instance
Service instances configured (2 in total):
Service instance 5:
Maintenance domain: md_5
Maintenance domain index: 5
Maintenance association: ma_5
Maintenance association index: 5
Level: 5 VLAN: 5 MIP rule: NONE CCM interval: 1s Direction: Inbound
MEP ID: 730 Interface: FortyGigE1/1/1

Service instance 6:
Maintenance domain: (Without ID)
Maintenance domain index: 6
Maintenance association: ma_6
Maintenance association index: 6
Level: 6 VLAN: 6 MIP rule: NONE CCM interval: 1s Direction: Outbound
MEP ID: 731 Interface: FortyGigE1/1/2
```

Table 20 Command output

| Field | Description |
|-----------------------------------|--|
| Service instances are configured. | Number of service instances configured. |
| Service instance | Service instance ID. |
| Maintenance domain | MD of the service instances. (If the MD does not have a name, this field displays Without ID .) |
| Maintenance domain index | Index of the MD to which the service instances belong. |
| Maintenance association: | MA of the service instances. |

| Field | Description |
|-------------------------------|---|
| Maintenance association index | Index of the MA to which the service instances belong. |
| Level | MD level. |
| VLAN | VLAN to which the MA belongs. |
| MIP rule | MIP generation rules configured on service instance. |
| CCM interval | Interval to send CCMs. |
| Direction | Direction of the MEPs configured on the service instance. |
| MEP ID | ID of MEPs configured on the service instance. |
| Interface | Interface of the MEP configured on the service instance. |

display cfd status

Use **display cfd status** to display the CFD and AIS status.

Syntax

display cfd status

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

```
# Display the CFD status.
<Sysname> display cfd status
CFD is enabled.
AIS is disabled.
```

display cfd tst

Use **display cfd tst** to display the TST result.

Syntax

display cfd tst [**service-instance** *instance-id* [**mep** *mep-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767. If you do not specify this option, the command displays the TST results for all service instances.

mep *mep-id*: Specifies a MEP by its ID in the range of 1 to 8191. If you do not specify this option, the command displays the TST results for all MEPs.

Usage guidelines

The TST DM results for all inward-facing MEPs in a service instance are the same.

Examples

```
# Display the TST results for all the MEPs in all service instances.
<Sysname> display cfd tst
Service instance: 1
MEP ID: 1003
Sent TST total number: 0
Received TST total number: 5
Received from 0010-fc00-6510, Bit True, sequence number 0
Received from 0010-fc00-6510, Bit True, sequence number 1
Received from 0010-fc00-6510, Bit True, sequence number 2
Received from 0010-fc00-6510, Bit True, sequence number 3
Received from 0010-fc00-6510, Bit True, sequence number 4
MEP ID: 1004
Sent TST total number: 5
Received TST total number: 0

Service instance: 2
No MEP exists in the service instance.

Service instance: 3
MEP ID: 1023
Sent TST total number: 5
Received TST total number: 0
```

Table 21 Command output

| Field | Description |
|---|--|
| Service instance | Service instance of the MEP. |
| Sent TST total number | Number of sent TST frames. |
| Received TST total number | Number of received TST frames. |
| Received from 0010-fc00-6510, Bit True, sequence number 0 | TST frame with sequence number 0 was received from the MEP with MAC address 0010-FC00-6510: <ul style="list-style-type: none">• Bit True—No bit error occurred.• Bit False—Bit errors occurred. |

Related commands

- **cfd tst**
- **reset cfd tst**

reset cfd dm one-way history

Use **reset cfd dm one-way history** to clear the one-way DM result.

Syntax

```
reset cfd dm one-way history [ service-instance instance-id [ mep mep-id ] ]
```

Views

User view

Predefined user roles

network-admin

Parameters

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767. If you do not specify this option, the command clears the one-way DM results for all service instances.

mep *mep-id*: Specifies a MEP by its ID in the range of 1 to 8191. If you do not specify this option, the command clears the one-way DM results for all MEPs.

Usage guidelines

Clearing the one-way DM result for an inward-facing MEP clears all one-way DM results for the service instance where the inward-facing MEP resides.

Examples

```
# Clear the one-way DM results for all MEPs in all service instances.  
<Sysname> reset cfd dm one-way history
```

Related commands

- **cfd dm one-way**
- **display cfd dm one-way history**

reset cfd tst

Use **reset cfd tst** to clear the TST result.

Syntax

```
reset cfd tst [ service-instance instance-id [ mep mep-id ] ]
```

Views

User view

Predefined user roles

network-admin

Parameters

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767. If you do not specify this option, the command clears the TST results for all service instances.

mep *mep-id*: Specifies a MEP by its ID in the range of 1 to 8191. If you do not specify this option, the command clears the TST results for all MEPs.

Usage guidelines

Clearing the TST result for an inward-facing MEP clears all TST results for the service instance where the inward-facing MEP resides.

Examples

Clear the TST results for all MEPs in all service instances.

```
<Sysname> reset cfd tst
```

Related commands

- **cfm tst**
- **display cfd tst**

DLDP commands

display dldp

Use **display dldp** to display DLDP configuration.

Syntax

```
display dldp [ interface interface-type interface-number ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

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

Usage guidelines

If no port is specified, this command displays global and port-specific DLDP configuration. If a port is specified, this command displays only the DLDP configuration on the port.

Examples

Display global and port-specific DLDP configuration.

```
<Sysname> display dldp
DLDP global status: Enabled
DLDP advertisement interval: 5s
DLDP authentication-mode: Simple
DLDP authentication-password: *****
DLDP unidirectional-shutdown mode: Auto
DLDP delaydown-timer value: 1s
Number of enabled ports: 2

Interface FortyGigE1/1/1
DLDP port state: Bidirectional
Number of the port's neighbors: 1
Neighbor MAC address: 0023-8956-3600
Neighbor port index: 79
Neighbor state: Confirmed
Neighbor aged time: 13s

Interface FortyGigE1/1/2
DLDP port state: Inactive
Number of the port's neighbors: 0 (Maximum number ever detected: 1)

# Display the DLDP configuration of FortyGigE 1/1/1.
```

```

<Sysname> display dldp interface fortygige 1/1/1
Interface FortyGigE1/1/1
  DLDAP port state: Bidirectional
  Number of the port's neighbors: 1
    Neighbor MAC address: 0023-8956-3600
    Neighbor port index: 79
    Neighbor state: Confirmed
    Neighbor aged time: 13s

```

Table 22 Command output

| Field | Description |
|-----------------------------------|---|
| DLDP global status | Global DLDP state (Enabled or Disabled). |
| DLDP advertisement interval | Interval for sending Advertisement packets (in seconds) to maintain neighbor relations. |
| DLDP authentication-mode | DLDP authentication mode (None, Simple, or md5). |
| DLDP authentication-password | Password for DLDP authentication: <ul style="list-style-type: none"> • *****—The password has been configured. • Not configured—The authentication mode has been configured but no password is configured. |
| DLDP unidirectional-shutdown mode | Port shutdown mode (Auto or Manual) after unidirectional links are detected. |
| DLDP delaydown-timer value | Setting of the DelayDown timer, in seconds. |
| Number of enabled ports | Number of the DLDP-enabled ports. |
| Interface | Index of a DLDP-enabled port. |
| DLDP port state | DLDP state on a port: <ul style="list-style-type: none"> • Bidirectional. • Inactive. • Initial. • Unidirectional. |
| Number of the port's neighbors | Current number of neighbors. |
| Maximum number ever detected | Maximum number of neighbors once detected on the port. This field appears only when the current number of neighbors is different from the maximum number of neighbors once detected. |
| Neighbor MAC address | MAC address of the neighbor. |
| Neighbor port index | Neighbor port index. |
| Neighbor state | Neighbor state (Confirmed or Unconfirmed). |
| Neighbor aged time | Neighbor aging time. |

display dldp statistics

Use **display dldp statistics** to display the statistics on the DLDP packets passing through a port.

Syntax

```
display dldp statistics [ interface interface-type interface-number ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

Usage guidelines

If no port is specified, this command displays the statistics on the DLDAP packets passing through all the DLDAP-enabled ports.

Examples

Display the statistics on the DLDAP packets passing through all the DLDAP-enabled ports.

```
<Sysname> display dldap statistics
Interface FortyGigE1/1/1
  Packets sent: 6
  Packets received: 5
  Invalid packets received: 2
  Loopback packets received: 0
  Authentication-failed packets received: 0
  Valid packets received: 3
```

```
Interface FortyGigE1/1/2
  Packets sent: 7
  Packets received: 7
  Invalid packets received: 3
  Loopback packets received: 0
  Authentication-failed packets received: 0
  Valid packets received: 4
```

Table 23 Command output

| Field | Description |
|--|--|
| Interface | Port index. |
| Packets sent | Total number of DLDAP packets sent. |
| Packets received | Total number of DLDAP packets received. |
| Invalid packets received | Number of the invalid packets received. |
| Loop packets received | Number of the loopback packets received. |
| Authentication failed packets received | Number of the received packets that failed to pass the authentication. |
| Valid packets received | Number of the valid packets received. |

Related commands

reset dldap statistics

lldp authentication-mode

Use **lldp authentication-mode** to configure DLDP authentication.

Use **undo lldp authentication-mode** to restore the default.

Syntax

```
lldp authentication-mode { md5 | none | simple }  
undo lldp authentication-mode
```

Default

DLDP authentication is not performed.

Views

System view

Predefined user roles

network-admin

Parameters

md5: Specifies the MD5 authentication mode.

none: Specifies not to perform authentication.

simple: Specifies the plain text authentication mode.

Usage guidelines

To enable DLDP to operate correctly, make sure the DLDP authentication modes and the passwords configured on the two ends of a link are the same.

If you do not configure the authentication password after you configure the authentication mode, the authentication mode is **none** no matter which authentication mode you configure.

Examples

Configure to perform plain text authentication and set the password to **abc** (assuming that Device A and Device B are connected by a DLDP link).

- Configure Device A:

```
<DeviceA> system-view  
[DeviceA] lldp authentication-mode simple  
[DeviceA] lldp authentication-password simple abc
```
- Configure Device B:

```
<DeviceB> system-view  
[DeviceB] lldp authentication-mode simple  
[DeviceB] lldp authentication-password simple abc
```

Related commands

- **display lldp**
- **lldp authentication-password**

lldp authentication-password

Use **lldp authentication-password** to configure the password for DLDP authentication.

Use **undo dldp authentication-password** to restore the default.

Syntax

```
dldp authentication-password { cipher cipher | simple simple }  
undo dldp authentication-password
```

Default

No DLDAP authentication password is configured.

Views

System view

Predefined user roles

network-admin

Parameters

cipher *cipher*: Sets a ciphertext password. The *cipher* argument is a case-sensitive string of 1 to 53 characters.

simple *simple*: Sets a plaintext password. The *simple* argument is a case-sensitive string of 1 to 16 characters.

Usage guidelines

For security purposes, all DLDAP authentication passwords, including passwords configured in plain text, are saved in cipher text.

To enable DLDAP to operate correctly, make sure the DLDAP authentication modes and the passwords configured on the two ends of a link are the same.

If you do not configure the authentication password after you configure the authentication mode, the authentication mode is **none** no matter which authentication mode you configure.

Examples

Configure to perform plain text authentication and set the password to **abc** (assuming that Device A and Device B are connected by a DLDAP link).

- Configure Device A:

```
<DeviceA> system-view  
[DeviceA] dldp authentication-mode simple  
[DeviceA] dldp authentication-password simple abc
```
- Configure Device B:

```
<DeviceB> system-view  
[DeviceB] dldp authentication-mode simple  
[DeviceB] dldp authentication-password simple abc
```

Related commands

- **display dldp**
- **dldp authentication-mode**

dldp delaydown-timer

Use **dldp delaydown-timer** to set the DelayDown timer.

Use **undo dldp delaydown-timer** to restore the default.

Syntax

```
dldp delaydown-timer time  
undo dldp delaydown-timer
```

Default

The setting of the DelayDown timer is 1 second.

Views

System view

Predefined user roles

network-admin

Parameters

time: Specifies the DelayDown timer in the range of 1 to 5 seconds.

Usage guidelines

The DelayDown timer configured by using this command applies to all DLDP-enabled ports.

Examples

```
# Set the DelayDown timer to 2 seconds.  
<Sysname> system-view  
[Sysname] dldp delaydown-timer 2
```

Related commands

```
display dldp
```

dldp enable

Use **dldp enable** to enable DLDP on a port.

Use **undo dldp enable** to disable DLDP on a port.

Syntax

```
dldp enable  
undo dldp enable
```

Default

DLDP is disabled on a port.

Views

Layer 2 Ethernet interface view, Layer 3 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

DLDP can take effect only after you enable it globally and on a port.

Examples

```
# Enable DLDP globally, and then enable DLDP on FortyGigE 1/1/1.  
<Sysname> system-view
```

```
[Sysname] dldp global enable
[Sysname] interface fortygige 1/1/1
[Sysname-FortyGigE1/1/1] dldp enable
```

Related commands

- **display dldp**
- **dldp global enable**

dldp global enable

Use **dldp global enable** to enable DLDP globally.

Use **undo dldp global enable** to disable DLDP globally.

Syntax

dldp global enable

undo dldp global enable

Default

DLDP is disabled globally.

Views

System view

Predefined user roles

network-admin

Usage guidelines

DLDP can take effect only after you enable it globally and on a port.

Examples

```
# Enable DLDP globally.
<Sysname> system-view
[Sysname] dldp global enable
```

Related commands

- **display dldp**
- **dldp enable**

dldp interval

Use **dldp interval** to set the interval for sending Advertisement packets.

Use **undo dldp interval** to restore the default.

Syntax

dldp interval *time*

undo dldp interval

Default

The interval for sending Advertisement packets is 5 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

time: Specifies Advertisement packets sending interval in the range of 1 to 100 seconds.

Usage guidelines

This command applies to all DLDAP-enabled ports.

To enable DLDAP to operate correctly, make sure the intervals for sending Advertisement packets configured on the two ends of a link are the same.

Examples

```
# Set the interval for sending Advertisement packets to 20 seconds.
<Sysname> system-view
[Sysname] dldp interval 20
```

Related commands

display dldp

dldp unidirectional-shutdown

Use **dldp unidirectional-shutdown** to set the port shutdown mode.

Use **undo dldp unidirectional-shutdown** to restore the default.

Syntax

```
dldp unidirectional-shutdown { auto | manual }
undo dldp unidirectional-shutdown
```

Default

The port shutdown mode is auto mode.

Views

System view

Predefined user roles

network-admin

Parameters

auto: Configures the port shutdown mode as auto mode. In this mode, when DLDAP detects a unidirectional link, it shuts down the Unidirectional port.

manual: Configures the port shutdown mode as manual mode. In this mode, when DLDAP detects a unidirectional link, DLDAP does not shut down the involved port but you need to manually shut it down. When the link state is restored to Bidirectional, you must manually bring up the port.

Examples

```
# Set the port shutdown mode to manual mode.
<Sysname> system-view
```

[Sysname] dldp unidirectional-shutdown manual

Related commands

display dldp

reset dldp statistics

Use **reset dldp statistics** to clear the statistics on DLDP packets passing through a port.

Syntax

reset dldp statistics [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Clears the statistics on DLDP packets passing through a port. *interface-type interface-number* represents a port by its type and number.

Usage guidelines

If no port is specified, this command clears the statistics on the DLDP packets passing through all the DLDP-enabled ports.

Examples

Clear the statistics on the DLDP packets passing through all the DLDP-enabled ports.

```
<Sysname> reset dldp statistics
```

Related commands

display dldp statistics

RRPP commands

control-vlan

Use **control-vlan** to configure the primary control VLAN for the RRPP domain.

Use **undo control-vlan** to remove the primary control VLAN from the RRPP domain.

Syntax

control-vlan *vlan-id*

undo control-vlan

Default

No control VLAN exists in the RRPP domain.

Views

RRPP domain view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies the ID of the primary control VLAN, in the range of 2 to 4093. The VLAN must have not been created yet.

Usage guidelines

When you configure control VLANs for an RRPP domain, you only need to configure the primary control VLAN. The system automatically configures the secondary control VLAN. It uses the primary control VLAN ID plus 1 as the secondary control VLAN ID. For the control VLAN configuration to succeed, make sure the IDs of the two control VLANs are consecutive and have not been assigned yet.

To ensure correct forwarding of RRPPDUs, follow these guidelines:

- Do not configure the default VLAN of a port accessing an RRPP ring as the control VLAN.
- Do not enable QinQ or VLAN mapping on the control VLANs.

After you configure RRPP rings for an RRPP domain, you cannot delete or modify the primary control VLAN of the domain. To do so, use the **undo control-vlan** command.

Examples

Configure VLAN 100 as the primary control VLAN of RRPP domain 1 (assume that VLAN 100 and VLAN 101 have not been created yet).

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
```

display rrpp brief

Use **display rrpp brief** to display brief RRPP information.

Syntax

display rrpp brief

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display brief RRPP information.

```
<Sysname> display rrpp brief
```

```
Flags for node mode: M -- Master, T -- Transit, E -- Edge, A -- Assistant-edge
```

```
RRPP protocol status: Enabled
```

```
Domain ID      : 1
```

```
Control VLAN   : Primary 5, Secondary 6
```

```
Protected VLAN: Reference instance 0 to 2, 4
```

```
Hello timer    : 1 seconds, Fail timer: 3 seconds
```

```
Fast detection status: Disabled
```

```
Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
```

```
Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms
```

| Ring ID | Ring level | Node mode | Primary/Common port | Secondary/Edge port | Enable status |
|---------|------------|-----------|---------------------|---------------------|---------------|
| 1 | 1 | M | FGE1/1/1 | FGE1/1/2 | Yes |

```
Domain ID      : 2
```

```
Control VLAN   : Primary 10, Secondary 11
```

```
Protected VLAN: Reference instance 0 to 2, 4
```

```
Hello timer    : 1 seconds, Fail timer: 3 seconds
```

```
Fast detection status: Disabled
```

```
Fast-Hello timer: 10 ms, Fast-Fail timer: 30 ms
```

| Ring ID | Ring level | Node mode | Primary/Common port | Secondary/Edge port | Enable status |
|---------|------------|-----------|---------------------|---------------------|---------------|
| 1 | 0 | T | FGE1/1/3 | FGE1/1/4 | Yes |

Table 24 Command output

| Field | Description |
|---------------------|--|
| RRPP node mode: | |
| Flags for node mode | <ul style="list-style-type: none">• M—Master node.• T—Transit node.• E—Edge node.• A—Assistant edge node. |

| Field | Description |
|-----------------------|--|
| RRPP protocol status | RRPP status: <ul style="list-style-type: none"> • Enabled—Globally enabled. • Disabled—Globally disabled. |
| Domain ID | RRPP domain ID. |
| Control VLAN | Primary and secondary control VLANs of the RRPP domain. |
| Protected VLAN | MSTIs corresponding to the VLANs protected by the RRPP domain. To view the VLAN-to-instance mappings, use the display stp region-configuration command (see <i>Layer 2—LAN Switching Command Reference</i>). |
| Hello timer | Hello timer value in seconds. |
| Fail timer | Fail timer value in seconds. |
| Fast detection status | Fast detection status: Enabled or Disabled . |
| Fast-Hello timer | Fast-Hello timer value in milliseconds. |
| Fast-Fail timer | Fast-Fail timer value in milliseconds. |
| Fast-Edge-Hello timer | Fast-Edge-Hello timer value in milliseconds. |
| Fast-Edge-Fail timer | Fast-Edge-Fail timer value in milliseconds. |
| Ring ID | RRPP ring ID. |
| Ring level | RRPP ring level: <ul style="list-style-type: none"> • 0—Primary ring. • 1—Subring. |
| Primary/Common port | <p>This field displays primary ports when the node mode is master node or transit node.</p> <p>This field displays common ports when the node mode is edge node or assistant edge node.</p> <p>A hyphen (-) appears when one of the following cases occurs:</p> <ul style="list-style-type: none"> • The port is not configured on the ring. • The card to which the port belongs has not started up. • The port is a member of a link aggregation group. |
| Secondary/Edge port | <p>This field displays secondary ports when the node mode is master node or transit node.</p> <p>This field displays edge ports when the node mode is edge node or assistant edge node.</p> <p>A hyphen (-) appears when one of the following cases occurs:</p> <ul style="list-style-type: none"> • The port is not configured on the ring. • The card to which the port belongs has not started up. • The port is a member of a link aggregation group. |
| Enable status | RRPP ring status: <ul style="list-style-type: none"> • Yes—Enabled. • No—Disabled. |

display rrpp ring-group

Use **display rrpp ring-group** to display the RRPP ring group configuration.

Syntax

```
display rrpp ring-group [ ring-group-id ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ring-group-id: Specifies an RRPP ring group by its ID in the range of 1 to 64. If you do not specify this argument, the command displays the configuration of all ring groups.

Usage guidelines

For an edge node RRPP ring group, this command also displays the subring sending Edge-Hello packets.

Examples

```
# Display the configuration of all RRPP ring groups.
```

```
<Sysname> display rrpp ring-group  
Ring group 1:  
  Domain 1 ring 1 to 3, 5  
  Domain 2 ring 1 to 3, 5  
  Domain 1 ring 1 is the sending ring  
  
Ring group 2:  
  Domain 1 ring 4, 6 to 7  
  Domain 2 ring 4, 6 to 7
```

Table 25 Command output

| Field | Description |
|-------------------------------------|--|
| Ring group 1 | RRPP ring group 1. |
| Domain 1 ring 1 to 3, 5 | Subrings in the ring group, including rings 1, 2, 3, and 5 in RRPP domain 1. |
| Domain 1 ring 1 is the sending ring | The sending ring of the ring group is ring 1 in RRPP domain 1. |

display rrpp statistics

Use **display rrpp statistics** to display RRPPDU statistics.

Syntax

```
display rrpp statistics domain domain-id [ ring ring-id ]
```


Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

domain *domain-id*: Specifies an RRPP domain by its ID in the range of 1 to 128.

ring *ring-id*: Specifies an RRPP ring by its ID in the range of 1 to 128. If you do not specify this option, the command displays the RRPPDU statistics for all rings in the specified RRPP domain.

Usage guidelines

If a port belongs to more than one ring, this command collects and displays RRPPDU statistics of the port by ring.

When a ring transits from inactive status to active status, packet counting for the ring restarts.

Examples

Display RRPPDU statistics for all rings in RRPP domain 2.

```
<Sysname> display rrpp statistics domain 2
Ring ID      : 1
Ring level   : 0
Node mode    : Master
Active status : Yes
Primary port  : FGE1/1/1
Fast-Hello packets: 0 Sent, 0 Received
Fast-Edge-Hello packets: 0 Sent, 0 Received
Direct Hello   Link      Common      Complete   Edge      Major      Total
                down      flush FDB   flush FDB  hello     fault
-----
Out   16924    0          0           1           0          0         16925
In     0         0          0           0           0          0          0
Secondary port: FGE1/1/2
Fast-Hello packets: 0 Sent, 0 Received
Fast-Edge-Hello packets: 0 Sent, 0 Received
Direct Hello   Link      Common      Complete   Edge      Major      Total
                down      flush FDB   flush FDB  hello     fault
-----
Out    0         0          0           0           0          0          0
In   16878    0          0           1           0          0         16879

Ring ID      : 2
Ring level   : 1
Node mode    : Edge
Active status : No
Common port  : FGE1/1/1
Fast-Hello packets: 0 Sent, 0 Received
Fast-Edge-Hello packets: 0 Sent, 0 Received
```

```

Direct Hello      Link      Common      Complete      Edge      Major      Total
                  down      flush FDB    flush FDB     hello     fault
-----
Out      0          0          0          0          0          0          0
In       0          0          0          0          0          0          0
Common port      : FGE1/1/2
Fast-Hello packets: 0 Sent, 0 Received
Fast-Edge-Hello packets: 0 Sent, 0 Received
Direct Hello      Link      Common      Complete      Edge      Major      Total
                  down      flush FDB    flush FDB     hello     fault
-----
Out      0          0          0          0          0          0          0
In       0          0          0          0          0          0          0
Edge port        : FGE1/1/3
Direct Hello      Link      Common      Complete      Edge      Major      Total
                  down      flush FDB    flush FDB     hello     fault
-----
Out      0          0          0          0          0          0          0
In       0          0          0          0          0          0          0

```

Table 26 Command output

| Field | Description |
|----------------|---|
| Ring ID | RRPP ring ID. |
| Ring level | RRPP ring level: <ul style="list-style-type: none"> • 0—Primary ring. • 1—Subring. |
| Node mode | Node mode: <ul style="list-style-type: none"> • Master node. • Transit node. • Edge node. • Assistant edge node. |
| Active status | RRPP ring status: <ul style="list-style-type: none"> • Yes—Active. • No—Inactive. |
| Primary port | The primary port field means the node mode is master node or transit node. A hyphen (-) appears when one of the following cases occurs: <ul style="list-style-type: none"> • The port is not configured on the ring. • The card to which the port belongs has not started up. • The port is a member of a link aggregation group. |
| Secondary port | The secondary port field means the node mode is master node or transit node. A hyphen (-) appears when one of the following cases occurs: <ul style="list-style-type: none"> • The port is not configured on the ring. • The card to which the port belongs has not started up. • The port is a member of a link aggregation group. |

| Field | Description |
|-------------------------|--|
| Common port | <p>The common port field means the node mode is edge node or assistant edge node.</p> <p>A hyphen (-) appears when one of the following cases occurs:</p> <ul style="list-style-type: none"> • The port is not configured on the ring. • The card to which the port belongs has not started up. • The port is a member of a link aggregation group. |
| Edge port | <p>The edge port field means the node mode is edge node or assistant edge node.</p> <p>A hyphen (-) appears when one of the following cases occurs:</p> <ul style="list-style-type: none"> • The port is not configured on the ring. • The card to which the port belongs has not started up. • The port is a member of a link aggregation group. |
| Fast-Hello packets | <p>Fast-Hello packet statistics on the port:</p> <ul style="list-style-type: none"> • Sent—Number of Fast-Hello packets sent out of the port. • Received—Number of Fast-Hello packets received on the port. |
| Fast-Edge-Hello packets | <p>Fast-Edge-Hello packet statistics on the port:</p> <ul style="list-style-type: none"> • Sent—Number of Fast-Edge-Hello packets sent out of the port. • Received—Number of Fast-Edge-Hello packets received on the port. |
| Packet direct | <p>Packet transmission direction on the port:</p> <ul style="list-style-type: none"> • Out—Packet sending direction. • In—Packet receiving direction. |
| Hello | Statistics of Hello packets received/sent on the port. |
| Link down | Statistics of Link-Down packets received/sent on the port. |
| Common flush FDB | Statistics of Common-Flush-FDB packets received/sent on the port. |
| Complete flush FDB | Statistics of Complete-Flush-FDB packets received/sent on the port. |
| Edge hello | Statistics of Edge-Hello packets received/sent on the port. |
| Major fault | Statistics of Major-Fault packets received/sent on the port. |
| Total | Total number of packets received/sent on the port. Only Hello, Link-Down, Common-Flush-FDB, Complete-Flush-FDB, Edge-Hello, and Major-Fault packets of RRPP are counted. |

Related commands

`reset rrpp statistics`

display rrpp verbose

Use `display rrpp verbose` to display detailed RRPP information.

Syntax

`display rrpp verbose domain domain-id [ring ring-id]`

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

domain *domain-id*: Specifies an RRPP domain by its ID in the range of 1 to 128.

ring *ring-id*: Specifies an RRPP ring by its ID in the range of 1 to 128. If you do not specify this option, the command displays detailed information for all rings in the specified RRPP domain.

Examples

Display detailed information for all rings in RRPP domain 2.

```
<Sysname> display rrpp verbose domain 2
Domain ID      : 2
Control VLAN   : Primary 10, Secondary 11
Protected VLAN: Reference instance 3, 5 to 7
Hello timer    : 1 seconds, Fail timer: 3 seconds
Fast detection status: Disabled
Fast-Hello timer: 20 ms, Fast-Fail timer: 60 ms
Fast-Edge-Hello timer: 10 ms, Fast-Edge-Fail timer: 30 ms

Ring ID        : 1
Ring level     : 0
Node mode      : Master
Ring state     : Completed
Enable status  : Yes, Active status: Yes
Primary port   : FGE1/1/2           Port status: UP
Secondary port : FGE1/1/3           Port status: BLOCKED

Ring ID        : 2
Ring level     : 1
Node mode      : Edge
Ring state     : -
Enable status  : No, Active status: No
Common port    : FGE1/1/2           Port status: -
                FGE1/1/3           Port status: -
Edge port      : FGE1/1/1           Port status: -
```

Table 27 Command output

| Field | Description |
|----------------|--|
| Domain ID | RRPP domain ID. |
| Control VLAN | Control VLANs of the RRPP domain: <ul style="list-style-type: none">• Primary—Primary control VLAN.• Secondary—Secondary control VLAN. |
| Protected VLAN | MSTIs corresponding to the VLANs protected by the RRPP domain. To view the VLAN-to-instance mappings, use the display stp region-configuration command (see <i>Layer 2—LAN Switching Command Reference</i>). |
| Hello timer | Hello timer value in seconds. |

| Field | Description |
|-----------------------|--|
| Fail timer | Fail timer value in seconds. |
| Fast detection status | Fast detection mechanism status: Enabled or Disabled . |
| Fast-Hello timer | Fast-Hello timer value in milliseconds. |
| Fast-Fail timer | Fast-Fail timer value in milliseconds. |
| Fast-Edge-Hello timer | Fast-Edge-Hello timer value in milliseconds. |
| Fast-Edge-Fail timer | Fast-Edge-Fail timer value in milliseconds. |
| Ring ID | RRPP ring ID. |
| Ring level | RRPP ring level: <ul style="list-style-type: none"> • 0—Primary ring. • 1—Subring. |
| Node mode | Node mode: <ul style="list-style-type: none"> • Master node. • Transit node. • Edge node. • Assistant edge node. |
| Ring state | RRPP ring state: <ul style="list-style-type: none"> • Completed—The ring is healthy. • Failed—The ring is not closed. <p>If the ring is not enabled on the device operating as the master node or the device is not the master node of the ring, a hyphen (-) is displayed.</p> |
| Enable status | RRPP ring status: <ul style="list-style-type: none"> • Yes—Enabled. • No—Disabled. |
| Active status | RRPP ring status. <ul style="list-style-type: none"> • Yes—Active. • No—Inactive. <p>An RRPP ring can be active only when RRPP and the RRPP ring are both enabled. This field also helps you identify whether RRPP is enabled.</p> |
| Primary port | The primary port field means the node mode is master node or transit node. A hyphen (-) appears when one of the following cases occurs: <ul style="list-style-type: none"> • The port is not configured on the ring. • The card to which the port belongs has not started up. • The port is a member of a link aggregation group. |
| Secondary port | The secondary port field means the node mode is master node or transit node. A hyphen (-) appears when one of the following cases occurs: <ul style="list-style-type: none"> • The port is not configured on the ring. • The card to which the port belongs has not started up. • The port is a member of a link aggregation group. |

| Field | Description |
|-------------|--|
| Common port | <p>The common port field means the node mode is edge node or assistant edge node.</p> <p>A hyphen (-) appears when one of the following cases occurs:</p> <ul style="list-style-type: none"> • The port is not configured on the ring. • The card to which the port belongs has not started up. • The port is a member of a link aggregation group. |
| Edge port | <p>The edge port field means the node mode is edge node or assistant edge node.</p> <p>A hyphen (-) appears when one of the following cases occurs:</p> <ul style="list-style-type: none"> • The port is not configured on the ring. • The card to which the port belongs has not started up. • The port is a member of a link aggregation group. |
| Port status | <p>Port status: Down, up, or blocked.</p> <p>A hyphen (-) appears when one of the following cases occurs:</p> <ul style="list-style-type: none"> • The ring is inactive. • The port is not configured on the ring. • The card to which the port belongs has not started up. • The port is a member of a link aggregation group. |

domain ring

Use **domain ring** to configure subbrings for an RRPP ring group.

Use **undo domain ring** to remove subbrings from the RRPP ring group.

Syntax

domain *domain-id* **ring** *ring-id-list*

undo domain *domain-id* [**ring** *ring-id-list*]

Default

No subring exists in the RRPP ring group.

Views

RRPP ring group view

Predefined user roles

network-admin

Parameters

domain-id: Specifies an RRPP domain by its ID in the range of 1 to 128.

ring *ring-id-list*: Specifies a space-separated list of up to 10 RRPP subring ID items. Each item specifies an RRPP subring ID or a range of RRPP subring IDs. The value range for RRPP subring IDs is 1 to 128. If you do not specify this option, the command removes all subbrings from the ring group in the specified domain.

Usage guidelines

Follow these guidelines when you configure an RRPP ring group on the edge node and the assistant edge node:

- When you assign an active ring to a ring group, assign it on the assistant edge node first and then on the edge node.
- To remove an active ring from a ring group, remove it on the edge node first and then on the assistant edge node.
- To remove the whole ring group, remove it on the edge node first and then on the assistant edge node.
- When you activate rings in a ring group, activate them on the edge node first and then on the assistant edge node.
- When you deactivate rings in a ring group, deactivate them on the assistant edge node first and then on the edge node.

If you do not follow these guidelines, the assistant edge node might fail to receive Edge-Hello packets and consider the primary ring failed even if it did not.

Examples

Create RRPP ring group 1, and add subrings 1, 2, 3, and 5 to domain 1 and domain 2.

```
<Sysname> system-view
[Sysname] rrpp ring-group 1
[Sysname-ring-group1] domain 1 ring 1 to 3 5
[Sysname-ring-group1] domain 2 ring 1 to 3 5
```

Related commands

- **display rrpp ring-group**
- **rrpp ring-group**

fast-detection enable

Use **fast-detection enable** to enable fast detection for the RRPP domain.

Use **undo fast-detection enable** to disable fast detection for the RRPP domain.

Syntax

fast-detection enable

undo fast-detection enable

Default

Fast detection is disabled for an RRPP domain.

Views

RRPP domain view

Predefined user roles

network-admin

Usage guidelines

To make fast detection take effect in an RRPP domain, enable fast detection, RRPP, and the RRPP rings in the RRPP domain.

When you configure fast detection for an RRPP domain, enable fast detection first on the edge node, and then on the assistant edge node. Otherwise, the assistant edge node might fail to receive Fast-Edge-Hello packets and consider the master node faulty even if it is not.

Examples

```
# Enable fast detection for RRPP domain 1.
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] fast-detection enable
```

Related commands

- **ring enable**
- **rrpp enable**

fast-edge-timer

Use **fast-edge-timer** to configure the Fast-Edge-Hello timer and the Fast-Edge-Fail timer.

Use **undo fast-edge-timer** to restore the default.

Syntax

fast-edge-timer hello-timer *hello-value* **fail-timer** *fail-value*

undo fast-edge-timer

Default

The Fast-Edge-Hello timer is 10 milliseconds and the Fast-Edge-Fail timer is 30 milliseconds.

Views

RRPP domain view

Predefined user roles

network-admin

Parameters

hello-timer *hello-value*: Specifies the Fast-Edge-Hello timer in the range of 5 to 100 milliseconds.

fail-timer *fail-value*: Specifies the Fast-Edge-Fail timer in the range of 15 to 300 milliseconds.

Usage guidelines

The Fast-Edge-Fail timer must be greater than or equal to three times the Fast-Edge-Hello timer.

Examples

```
# Set the Fast-Edge-Hello timer to 20 milliseconds and the Fast-Edge-Fail timer to 70 milliseconds for
RRPP domain 1.
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] fast-edge-timer hello-timer 20 fail-timer 70
```

fast-timer

Use **fast-timer** to configure the Fast-Hello timer and the Fast-Fail timer.

Use **undo fast-timer** to restore the default.

Syntax

fast-timer hello-timer *hello-value* **fail-timer** *fail-value*

undo fast-timer

Default

The Fast-Hello timer is 20 milliseconds and the Fast-Fail timer is 60 milliseconds.

Views

RRPP domain view

Predefined user roles

network-admin

Parameters

hello-timer *hello-value*: Specifies the Fast-Hello timer in the range of 10 to 500 milliseconds.

fail-timer *fail-value*: Specifies the Fast-Fail timer in the range of 30 to 1500 milliseconds.

Usage guidelines

The Fast-Fail timer must be greater than or equal to three times the Fast-Hello timer.

Examples

```
# Set the Fast-Hello timer to 20 milliseconds and the Fast-Fail timer to 70 milliseconds for RRPP domain 1.
```

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

```
[Sysname] rrpp domain 1
```

```
[Sysname-rrpp-domain1] fast-timer hello-timer 20 fail-timer 70
```

protected-vlan

Use **protected-vlan** to configure the protected VLANs for the RRPP domain.

Use **undo protected-vlan** to remove the protected VLANs from the RRPP domain.

Syntax

protected-vlan reference-instance *instance-id-list*

undo protected-vlan [**reference-instance** *instance-id-list*]

Default

No protected VLAN is configured for an RRPP domain.

Views

RRPP domain view

Predefined user roles

network-admin

Parameters

reference-instance *instance-id-list*: Specifies the Multiple Spanning Tree Instances (MSTIs) you want to reference in the form of *instance-id-list* = { *instance-id* [**to** *instance-id*] }&<1-10>. The *instance-id* argument is an MSTI ID in the range of 0 to 4094. You can specify up to 10 MSTI IDs or ID ranges. You can use the **display stp region-configuration** command to display the VLAN-to-instance mappings. If you do not specify this option, the command removes all MSTIs referenced by the RRPP domain.

Usage guidelines

You can delete or modify the protected VLANs configured for an RRPP domain before and after you configure rings for it. However, you cannot delete configurations of all the protected VLANs configured for the domain.

When the VLAN-to-instance mappings change, the protected VLANs of an RRPP domain also change.

Examples

```
# Map VLANs 1 through 30 to MSTI 1, and activate the MST region configuration. Configure VLAN 100 as the control VLAN of RRPP domain 1. Configure VLANs mapped to MSTI 1 as the primary control VLANs of RRPP domain 1.
```

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] instance 1 vlan 1 to 30
[Sysname-mst-region] active region-configuration
[Sysname-mst-region] quit
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protected-vlan reference-instance 1
```

Related commands

- **display stp region-configuration** (*Layer 2—LAN Switching Command Reference*)
- **rrpp domain**

reset rrpp statistics

Use **reset rrpp statistics** to clear RRPPDU statistics.

Syntax

```
reset rrpp statistics domain domain-id [ ring ring-id ]
```

Views

User view

Predefined user roles

network-admin

Parameters

domain *domain-id*: Specifies an RRPP domain by its ID in the range of 1 to 128.

ring *ring-id*: Specifies an RRPP ring by its ID in the range of 1 to 128. If you do not specify this option, the command clears RRPPDU statistics of all RRPP rings in the specified RRPP domain.

Examples

```
# Clear the RRPPDU statistics of ring 10 in RRPP domain 1.
<Sysname> reset rrpp statistics domain 1 ring 10
```

Related commands

display rrpp statistics

ring

Use **ring** to configure the node mode of the device, the role of the specified RRPP port, and the level of the RRPP ring.

Use **undo ring** to delete the RRPP ring.

Syntax

```
ring ring-id node-mode { { master | transit } [ primary-port interface-type interface-number ]  
[ secondary-port interface-type interface-number ] level level-value | { assistant-edge | edge }  
[ edge-port interface-type interface-number ] }
```

```
undo ring ring-id
```

Default

The device is not a node of the RRPP ring.

Views

RRPP domain view

Predefined user roles

network-admin

Parameters

ring-id: Specifies an RRPP ring by its ID in the range of 1 to 128.

master: Specifies the device as the master node of the RRPP ring.

transit: Specifies the device as the transit node of the RRPP ring.

primary-port: Specifies the port as a primary port.

interface-type interface-number: Specifies a port by its type and number.

secondary-port: Specifies the port as a secondary port.

level level-value: Specifies an RRPP ring level, 0 for the primary ring and 1 for the subring.

assistant-edge: Specifies the device as the assistant edge node of the RRPP ring.

edge: Specifies the device as the edge node of the RRPP ring.

edge-port: Specifies the edge port for the node.

Usage guidelines

The ID of an RRPP ring in a domain must be unique.

When an RRPP ring is activated, you cannot configure its RRPP ports.

When you configure the edge node and the assistant edge node, first configure the primary ring, and then the subrings.

The node mode, RRPP port role, and ring level settings of an RRPP ring cannot be modified after they are configured. To modify the settings, first remove the current settings.

Remove all subring configurations before you delete the primary ring configuration of the edge node or the assistant edge node. However, an active RRPP ring cannot be deleted.

When RRPP is enabled on a device, you must disable the RRPP ring before you can delete it. When RRPP is disabled on the device, you can directly delete the RRPP ring, as well as the setting of the **ring enable** command.

Examples

Specify the device as the master node of primary ring 10 in RRPP domain 1. Specify FortyGigE 1/1/1 as the primary port and FortyGigE 1/1/2 as the secondary port.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protected-vlan reference-instance 0 1 2
[Sysname-rrpp-domain1] ring 10 node-mode master primary-port fortygige 1/1/1
secondary-port fortygige 1/1/2 level 0
```

Specify the device as the transit node of primary ring 10 in RRPP domain 1. Specify FortyGigE 1/1/1 as the primary port and FortyGigE 1/1/2 as the secondary port. Specify the device as the edge node of subring 20 in RRPP domain 1, and specify FortyGigE 1/1/3 as the edge port.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protected-vlan reference-instance 0 1 2
[Sysname-rrpp-domain1] ring 10 node-mode transit primary-port fortygige 1/1/1
secondary-port fortygige 1/1/2 level 0
[Sysname-rrpp-domain1] ring 20 node-mode edge edge-port fortygige 1/1/3
```

Related commands

ring enable

ring enable

Use **ring enable** to enable an RRPP ring.

Use **undo ring enable** to disable the RRPP ring.

Syntax

ring *ring-id* **enable**

undo ring *ring-id* **enable**

Default

The RRPP ring is disabled.

Views

RRPP domain view

Predefined user roles

network-admin

Parameters

ring-id: Specifies an RRPP ring by its ID in the range of 1 to 128.

Usage guidelines

To activate an RRPP ring, you must enable RRPP and the RRPP ring.

Before you enable subrings on a device, you must enable the primary ring. Before you disable the primary ring on the device, you must disable all subrings. Otherwise, the system displays error prompts.

Examples

```
# Enable RRPP ring 10 in RRPP domain 1.
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protected-vlan reference-instance 0 1 2
[Sysname-rrpp-domain1] ring 10 node-mode master primary-port fortygige 1/1/1
secondary-port fortygige 1/1/2 level 0
[Sysname-rrpp-domain1] ring 10 enable
```

Related commands

rrpp enable

rrpp domain

Use **rrpp domain** to create an RRPP domain and enter its view.

Use **undo rrpp domain** to remove an RRPP domain.

Syntax

```
rrpp domain domain-id
undo rrpp domain domain-id
```

Default

No RRPP domain is created.

Views

System view

Predefined user roles

network-admin

Parameters

domain-id: Specifies an RRPP domain by its ID in the range of 1 to 128.

Usage guidelines

When you delete an RRPP domain, configurations of the control VLANs and protected VLANs are deleted at the same time.

To delete an RRPP domain successfully, make sure it has no RRPP rings.

Examples

```
# Create RRPP domain 1, and enter RRPP domain 1 view.
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1]
```

Related commands

- **control-vlan**

- **protected-vlan**

rrpp enable

Use **rrpp enable** to enable RRPP.

Use **undo rrpp enable** to disable RRPP.

Syntax

rrpp enable

undo rrpp enable

Default

RRPP is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

To activate the RRPP domain, enable RRPP and the RRPP rings for the RRPP domain.

Examples

```
# Enable RRPP.  
<Sysname> system-view  
[Sysname] rrpp enable
```

Related commands

ring enable

rrpp ring-group

Use **rrpp ring-group** to create an RRPP ring group and enter its view.

Use **undo rrpp ring-group** to remove an RRPP ring group.

Syntax

rrpp ring-group *ring-group-id*

undo rrpp ring-group *ring-group-id*

Default

No RRPP ring group is created.

Views

System view

Predefined user roles

network-admin

Parameters

ring-group-id: Specifies an RRPP ring group ID in the range of 1 to 64.

Usage guidelines

When you remove a ring group, remove it on the edge node first and then on the assistant edge node. Otherwise, the assistant edge node might fail to receive Edge-Hello packets and consider the primary ring failed even if it is not.

After a ring group is removed, all subrings in the ring group do not belong to any ring group.

Examples

```
# Create RRPP ring group 1 and enter its view.
<Sysname> system-view
[Sysname] rrpp ring-group 1
[Sysname-ring-group1]
```

Related commands

- **display rrpp ring-group**
- **domain ring**

timer

Use **timer** to configure the Hello timer and the Fail timer.

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

Syntax

```
timer hello-timer hello-value fail-timer fail-value
undo timer
```

Default

The Hello timer is 1 second and the Fail timer is 3 seconds.

Views

RRPP domain view

Predefined user roles

network-admin

Parameters

hello-timer *hello-value*: Specifies the Hello timer in the range of 1 to 10 seconds.

fail-timer *fail-value*: Specifies the Fail timer in the range of 3 to 30 seconds.

Usage guidelines

The Fail timer must be greater than or equal to three times the Hello timer.

Examples

```
# Set the Hello timer to 2 seconds and the Fail timer to 7 seconds for RRPP domain 1.
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] timer hello-timer 2 fail-timer 7
```

Smart Link commands

display smart-link flush

Use **display smart-link flush** to display information about the received flush messages.

Syntax

```
display smart-link flush
```

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about the received flush messages.

```
<Sysname> display smart-link flush
Received flush packets                : 10
Receiving interface of the last flush packet : FortyGigE1/1/1
Receiving time of the last flush packet   : 19:19:03 2014/04/21
Device ID of the last flush packet       : 000f-e200-8500
Control VLAN of the last flush packet    : 1
```

Table 28 Command output

| Field | Description |
|--|--|
| Received flush packets | Total number of received flush messages. |
| Receiving interface of the last flush packet | Port that received the last flush message. |
| Receiving time of the last flush packet | Time when the last flush message was received. |
| Device ID of the last flush packet | Device ID carried in the last flush message. |
| Control VLAN of the last flush packet | Control VLAN ID carried in the last flush message. |

Related commands

reset smart-link statistics

display smart-link group

Use **display smart-link group** to display information about the specified or all smart link groups.

Syntax

```
display smart-link group { group-id | all }
```


Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

group-id: Specifies a smart link group by its ID. The value range for the *group-id* argument is 1 to 48.

all: Displays information about all smart link groups.

Usage guidelines

If you configure a port as both an aggregation group member and a smart link group member, only the aggregation group configuration takes effect. The port is not shown in the output from the **display smart-link group** command. The smart link group configuration takes effect after the port leaves the aggregation group.

Examples

```
# Display information about smart link group 1.
```

```
<Sysname> display smart-link group 1
```

```
Smart link group 1 information:
```

```
Device ID       : 0011-2200-0001
```

```
Preemption mode : NONE
```

```
Preemption delay: 1(s)
```

```
Control VLAN    : 1
```

```
Protected VLAN  : Reference Instance 2, 4
```

| Member | Role | State | Flush-count | Last-flush-time |
|----------|-----------|---------|-------------|---------------------|
| FGE1/1/1 | PRIMARY | ACTIVE | 1 | 16:45:20 2014/04/21 |
| FGE1/1/2 | SECONDARY | STANDBY | 2 | 16:37:20 2014/04/21 |

Table 29 Command output

| Field | Description |
|--------------------------------|--|
| Smart link group 1 information | Information about smart link group 1. |
| Preemption mode | Preemption mode, which can be ROLE for preemption enabled or NONE for preemption disabled. |
| Preemption delay | Preemption delay time, in seconds. |
| Control-VLAN | Control VLAN ID. |
| Protected VLAN | Protected VLANs of the smart link group. Referenced Multiple Spanning Tree Instances (MSTIs) are displayed. To view the VLANs mapped to the referenced MSTIs, use the display stp region-configuration command. |
| Member | Member port of the smart link group. |
| Role | Port role: primary or secondary. |
| State | Port state: active, down, or standby. |

| Field | Description |
|-----------------|---|
| Flush-count | Number of transmitted flush messages. |
| Last-flush-time | Time when the last flush message was transmitted (NA indicates that no flush message has been transmitted). |

flush enable

Use **flush enable** to enable flush update.

Use **undo flush enable** to disable flush update.

Syntax

flush enable [**control-vlan** *vlan-id*]

undo flush enable

Default

Flush update is enabled for smart link groups, and VLAN 1 is used for flush message transmission.

Views

Smart link group view

Predefined user roles

network-admin

Parameters

control-vlan *vlan-id*: Specifies the control VLAN used for transmitting flush messages. The *vlan-id* argument represents the control VLAN ID in the range of 1 to 4094.

Usage guidelines

You must configure different control VLANs for different smart link groups.

- Make sure the configured control VLAN already exists, and assign the smart link group member ports to the control VLAN.
- The control VLAN of a smart link group must also be one of its protected VLANs. Do not remove the control VLAN. Otherwise, flush messages cannot be sent correctly.

Examples

```
# Disable flush update for smart link group 1.
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] undo flush enable
```

Related commands

smart-link flush enable

port

Use **port** to assign the specified port as the primary or secondary port of the current smart link group.

Use **undo port** to remove the specified port from the smart link group.

Syntax

```
port interface-type interface-number { primary | secondary }
```

```
undo port interface-type interface-number
```

Default

A smart link group has no member ports.

Views

Smart link group view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies a port by its type and number, which can be a Layer 2 Ethernet interface or Layer 2 aggregate interface.

primary: Specifies a port as the primary port.

secondary: Specifies a port as the secondary port.

Usage guidelines

Disable the spanning tree feature and RRPP on the ports you want to add to the smart link group. You cannot enable the spanning tree feature or RRPP on a smart link group member port.

If you configure a port as both an aggregation group member and a smart link group member, only the aggregation group configuration takes effect. The port is not shown in the output from the **display smart-link group** command. The smart link group configuration takes effect after the port leaves the aggregation group.

You can also assign a port to a smart link group by using the **port smart-link group** command in interface view.

Examples

```
# Configure FortyGigE 1/1/1 as the secondary port of smart link group 1.
```

```
<Sysname> system-view
[Sysname] interface fortygige 1/1/1
[Sysname-FortyGigE1/1/1] undo stp enable
[Sysname-FortyGigE1/1/1] quit
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 0
[Sysname-smlk-group1] port fortygige 1/1/1 secondary
```

Related commands

```
port smart-link group
```

port smart-link group

Use **port smart-link group** to configure the current port as a member of the specified smart link group.

Use **undo port smart-link group** to remove the port from the specified smart link group.

Syntax

```
port smart-link group group-id { primary | secondary }
```

undo port smart-link group *group-id*

Default

A port is not a smart link group member.

Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

group-id: Specifies a smart link group ID in the range of 1 to 48.

primary: Specifies the port as the primary port.

secondary: Specifies the port as the secondary port.

Usage guidelines

Disable the spanning tree feature and RRPP on the ports you want to add to the smart link group. You cannot enable the spanning tree feature or RRPP on a smart link group member port.

If you configure a port as both an aggregation group member and a smart link group member, only the aggregation group configuration takes effect. The port is not shown in the output from the **display smart-link group** command. The smart link group configuration takes effect after the port leaves the aggregation group.

You can assign a port to a smart link group by using the **port** command in smart link group view.

Examples

Configure FortyGigE 1/1/1 as the primary port of smart link group 1.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 0
[Sysname-smlk-group1] quit
[Sysname] interface fortygige 1/1/1
[Sysname-FortyGigE1/1/1] undo stp enable
[Sysname-FortyGigE1/1/1] port smart-link group 1 primary
```

Configure Layer 2 aggregate interface 1 as the primary port of smart link group 1.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 0
[Sysname-smlk-group1] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] undo stp enable
[Sysname-Bridge-Aggregation1] port smart-link group 1 primary
```

Related commands

port

port smart-link group track

Use **port smart-link group track** to configure the collaboration between a smart link group member port and a track entry.

Use **undo port smart-link group track** to remove the collaboration.

Syntax

port smart-link group *group-id* **track** *track-entry-number*

undo port smart-link group *group-id* **track** *track-entry-number*

Default

Smart link group member ports do not collaborate with any track entry.

Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

group-id: Specifies a smart link group ID in the range of 1 to 48.

track-entry-number: Specifies the ID of a track entry that has been associated with the CC function of CFD.

Usage guidelines

Smart Link collaborates with link detection protocols through track entries. It supports only the CC function of CFD to implement link detection. To associate the CC function of CFD with a track entry, use the **track cfd** command.

Before configuring the collaboration between Smart Link and Track on a port, make sure the port has been added to the specified smart link group.

Examples

Configure the collaboration between FortyGigE 1/1/1, the primary port of smart link group 1, and the CC function of CFD through track entry 1 to detect the link status.

```
<Sysname> system-view
[Sysname] track 1 cfd cc service-instance 100 mep 2
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 0
[Sysname-smlk-group1] quit
[Sysname] interface fortygige 1/1/1
[Sysname-FortyGigE1/1/1] undo stp enable
[Sysname-FortyGigE1/1/1] port smart-link group 1 primary
[Sysname-FortyGigE1/1/1] port smart-link group 1 track 1
```

Configure the collaboration between bridge-aggregation 1, the primary port of smart link group 1, and the CC function of CFD through track entry 1 to detect the link status.

```
<Sysname> system-view
[Sysname] track 1 cfd cc service-instance 100 mep 2
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 0
```

```
[Sysname-smlk-group1] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] undo stp enable
[Sysname-Bridge-Aggregation1] port smart-link group 1 primary
[Sysname-Bridge-Aggregation1] port smart-link group 1 track 1
```

Related commands

track cfd

preemption delay

Use **preemption delay** to set the preemption delay.

Use **undo preemption delay** to restore the default.

Syntax

preemption delay *delay*

undo preemption delay

Default

The preemption delay is 1 second.

Views

Smart link group view

Predefined user roles

network-admin

Parameters

delay: Specifies the preemption delay in the range of 0 to 300 seconds.

Usage guidelines

The preemption delay configuration takes effect only after role preemption is enabled.

When role preemption is enabled, and after the preemption delay is set, the primary port waits for a specific period before taking over in order to collaborate with the switchover of upstream devices.

Examples

```
# Enable role preemption and set the preemption delay to 10 seconds.
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] preemption mode role
[Sysname-smlk-group1] preemption delay 10
```

Related commands

preemption mode

preemption mode

Use **preemption mode** to enable role preemption.

Use **undo preemption mode** to disable role preemption.

Syntax

preemption mode role
undo preemption mode

Default

Role preemption is disabled.

Views

Smart link group view

Predefined user roles

network-admin

Parameters

role: Configures the role preemption mode, which enables the primary port to preempt the secondary port in active state.

Examples

```
# Enable the role preemption mode.
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] preemption mode role
```

protected-vlan

Use **protected-vlan** to configure protected VLANs for a smart link group.

Use **undo protected-vlan** to remove the protected VLAN configuration of the smart link group.

Syntax

protected-vlan reference-instance *instance-id-list*
undo protected-vlan [**reference-instance** *instance-id-list*]

Default

No protected VLAN is configured for a smart link group.

Views

Smart link group view

Predefined user roles

network-admin

Parameters

reference-instance *instance-id-list*: Specifies the MSTIs to be referenced in the form of *instance-id-list* = { *instance-id* [**to** *instance-id*] }&<1-10>, where *instance-id* is an MSTI ID in the range of 0 to 4094. An MSTI ID of 0 represents the common internal spanning tree (CIST). &<1-10> means that you can specify up to 10 MSTI IDs or ID ranges. You can use the **display stp region-configuration** command to display the instance-to-VLAN mappings.

Usage guidelines

If the **reference-instance** *instance-id-list* option is specified, the **undo protected-vlan** command removes configuration of VLANs mapped to the specified MSTIs. Otherwise, the command removes configuration of all protected VLANs.

Before assigning ports to a smart link group, configure protected VLANs for the smart link group.

You can remove the protected VLAN configuration of a smart link group when the group is empty but not after a member port is assigned to it.

Removing a smart link group also removes its protected VLAN configuration.

If the VLANs mapped to a referenced MSTI change, the protected VLANs also change.

The VLANs to which the member ports of a smart link group belong must be configured as the protected VLANs of the smart link group.

Examples

```
# Map VLANs 1 through 30 to MSTI 1, activate the MST region configuration, and configure the VLANs mapped to MSTI 1 as the protected VLANs of smart link group 1.
```

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] instance 1 vlan 1 to 30
[Sysname-mst-region] active region-configuration
[Sysname-mst-region] quit
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 1
```

Related commands

- **display stp region-configuration** (*Layer 2—LAN Switching Command Reference*)
- **smart-link group**

reset smart-link statistics

Use **reset smart-link statistics** to clear the statistics about flush messages.

Syntax

```
reset smart-link statistics
```

Views

User view

Predefined user roles

network-admin

Examples

```
# Clear the statistics about flush messages.
<Sysname> reset smart-link statistics
```

Related commands

```
display smart-link flush
```


smart-link flush enable

Use **smart-link flush enable** to enable the flush message receiving function.

Use **undo smart-link flush enable** to remove the configuration.

Syntax

smart-link flush enable [**control-vlan** *vlan-id-list*]

undo smart-link flush enable [**control-vlan** *vlan-id-list*]

Default

Flush messages are not processed.

Views

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

control-vlan *vlan-id-list*: Specifies the control VLANs used for receiving flush messages. The default is 1. The *vlan-id-list* is expressed in the form of *vlan-id-list* = { *vlan-id* [**to** *vlan-id*] }&<1-10>, where the *vlan-id* argument represents the ID of a control VLAN in the range of 1 to 4094. &<1-10> indicates that you can provide up to 10 VLAN IDs or VLAN ID lists.

Examples

Enable FortyGigE 1/1/1 to process the flush messages received in VLAN 1.

```
<Sysname> system-view
[Sysname] interface fortygige 1/1/1
[Sysname-FortyGigE1/1/1] smart-link flush enable
```

Enable Layer 2 aggregate interface 1 to process the flush messages received in VLAN 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] smart-link flush enable
```

Related commands

flush enable

smart-link group

Use **smart-link group** to create a smart link group and enter smart link group view.

Use **undo smart-link group** to remove a smart link group.

Syntax

smart-link group *group-id*

undo smart-link group *group-id*

Views

System view

Predefined user roles

network-admin

Parameters

group-id: Specifies a smart link group ID in the range of 1 to 48.

Usage guidelines

You cannot remove a smart link group with member ports.

Examples

Create smart link group 1 and enter smart link group view.

```
<Sysname> system-view  
[Sysname] smart-link group 1  
[Sysname-smk-group1]
```

Monitor Link commands

display monitor-link group

Use **display monitor-link group** to display monitor link group information.

Syntax

```
display monitor-link group { group-id | all }
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

group-id: Specifies a monitor link group by its ID. The value range for the *group-id* argument is 1 to 16.

all: Specifies all monitor link groups.

Usage guidelines

This command does not display information about ports that belong to a link aggregation group.

Examples

```
# Display information about monitor link group 1.
```

```
<Sysname> display monitor-link group 1
```

```
Monitor link group 1 information:
```

```
Group status      : UP  
Downlink up-delay: 0(s)  
Last-up-time     : 16:38:26 2014/4/21  
Last-down-time   : 16:37:20 2014/4/21
```

```
Member           Role      Status  
-----  
FGE1/1/1         UPLINK   UP  
FGE1/1/2         DOWNLINK UP
```

Table 30 Command output

| Field | Description |
|----------------------------------|--|
| Monitor link group 1 information | Information about monitor link group 1. |
| Group status | Monitor link group state, which can be up or down. |
| Downlink up-delay | Switchover delay of the downlink interfaces in the monitor link group, in seconds. |
| Last-up-time | Last time when the monitor link group was up. |

| Field | Description |
|----------------|--|
| Last-down-time | Last time when the monitor link group was down. |
| Member | Member interfaces of the monitor link group. |
| Role | Interface role, which can be uplink interface or downlink interface. |
| Status | Member link state, which can be up or down. |

downlink up-delay

Use **downlink up-delay** to configure the switchover delay for the downlink interfaces in a monitor link group.

Use **undo downlink up-delay** to restore the default.

Syntax

downlink up-delay *delay*

undo downlink up-delay

Default

The switchover delay for the downlink interfaces is 0 seconds. The downlink interfaces come up as soon as an uplink interface in the monitor link group comes up.

Views

Monitor link group view

Predefined user roles

network-admin

Parameters

delay: Specifies the switchover delay in the range of 1 to 300 seconds.

Usage guidelines

To avoid frequent state changes of downlink interfaces in the event that the uplink interfaces in the monitor link group flap, you can configure a switchover delay. After the switchover delay is configured, the downlink interfaces remain down until an uplink interface remains up for a period of time.

Examples

```
# Configure the switchover delay for the downlink interfaces in monitor link group 1 as 50 seconds.
<Sysname> system-view
[Sysname] monitor-link group 1
[Sysname-mtlk-group1] downlink up-delay 50
```

monitor-link group

Use **monitor-link group** to create a monitor link group and enter monitor link group view.

Use **undo monitor-link group** to remove a monitor link group.

Syntax

```
monitor-link group group-id  
undo monitor-link group group-id
```

Default

No monitor link group is created.

Views

System view

Predefined user roles

network-admin

Parameters

group-id: Specifies a monitor link group by its ID. The value range for the *group-id* argument is 1 to 16.

Examples

```
# Create monitor link group 1 and enter the view of monitor link group 1.  
<Sysname> system-view  
[Sysname] monitor-link group 1  
[Sysname-mtlk-group1]
```

port

Use **port** to assign an interface to the monitor link group.

Use **undo port** to remove an interface from the monitor link group.

Syntax

```
port interface-type { interface-number | interface-number.subnumber } { downlink | uplink }  
undo port interface-type interface-number
```

Default

A monitor link group has no member interfaces.

Views

Monitor link group view

Predefined user roles

network-admin

Parameters

interface-type: Specifies an interface type, which can be Layer 2 Ethernet interface, Layer 3 Ethernet interface, Layer 3 Ethernet subinterface, Layer 2 aggregate interface, Layer 3 aggregate interface, Layer 3 aggregate subinterface, member port of a Layer 2 aggregation group or Layer 3 aggregation group, S-channel interface, and S-channel aggregate interface.

interface-number: Specifies an interface by its number.

interface-number.subnumber: Specifies a subinterface by its number. The argument *subnumber* is in the range of 1 to 4094.

downlink: Specifies a downlink interface.

uplink: Specifies an uplink interface.

Usage guidelines

If you have configured an interface as the downlink interface of a monitor link group, do not configure its subinterfaces as the uplink interfaces of any monitor link group. Otherwise, the Monitor Link operation might be interrupted.

To avoid interrupting Monitor Link operation, do not assign the aggregate interface and member ports of an aggregate group to the same monitor link group.

The state of subinterfaces adapts to the state of the interface. Do not assign the interface and its subinterfaces to the same monitor link group. Otherwise, the monitor link group performance might be affected.

You can assign an interface to only one monitor link group.

You can also assign an interface to a monitor link group by using the **port monitor-link group** command in interface view.

Examples

```
# Configure FortyGigE 1/1/1 as an uplink interface and FortyGigE 1/1/2 as a downlink interface for monitor link group 1.
```

```
<Sysname> system-view
[Sysname] monitor-link group 1
[Sysname-mtlk-group1] port fortygige 1/1/1 uplink
[Sysname-mtlk-group1] port fortygige 1/1/2 downlink
```

Related commands

port monitor-link group

port monitor-link group

Use **port monitor-link group** to assign the current interface to a monitor link group as a member interface.

Use **undo port monitor-link group** to remove the current interface from a monitor link group.

Syntax

```
port monitor-link group group-id { downlink | uplink }
```

```
undo port monitor-link group group-id
```

Default

The interface/subinterface is not a monitor link group member.

Views

Layer 2 Ethernet interface view

Layer 3 Ethernet interface/subinterface view

Layer 2 aggregate interface view

Layer 3 aggregate interface/subinterface view

Layer 2 aggregation group member port view

Layer 3 aggregation group member port view

S-channel interface/S-channel aggregate interface view

Predefined user roles

network-admin

Parameters

group-id: Specifies a monitor link group by its ID. The value range for the *group-id* argument is 1 to 16.

downlink: Specifies a downlink interface.

uplink: Specifies an uplink interface.

Usage guidelines

If you have configured an interface as the downlink interface of a monitor link group, do not configure its subinterfaces as the uplink interfaces of any monitor link group. Otherwise, the Monitor Link operation might be interrupted.

To avoid interrupting Monitor Link operation, do not assign the aggregate interface and member ports of an aggregate group to the same monitor link group.

The state of subinterfaces adapts to the state of the interface. Do not assign the interface and its subinterfaces to the same monitor link group. Otherwise, the monitor link group performance might be affected.

You can assign an interface to only one monitor link group.

You can also assign an interface to a monitor link group with the **port** command in monitor link group view.

Examples

Configure FortyGigE 1/1/1 as an uplink interface and FortyGigE 1/1/2 as a downlink interface for monitor link group 1.

```
<Sysname> system-view
[Sysname] monitor-link group 1
[Sysname-mtlk-group1] quit
[Sysname] interface fortygige 1/1/1
[Sysname-FortyGigE1/1/1] port monitor-link group 1 uplink
[Sysname-FortyGigE1/1/1] quit
[Sysname] interface fortygige 1/1/2
[Sysname-FortyGigE1/1/2] port monitor-link group 1 downlink
```

Related commands

port

VRRP commands

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

VRRP cannot be configured on member ports of aggregation groups.

IPv4 VRRP commands

display vrrp

Use **display vrrp** to display the states of IPv4 VRRP groups.

Syntax

```
display vrrp [ interface interface-type interface-number [ vrid virtual-router-id ] ] [ verbose ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

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

vrid *virtual-router-id*: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

verbose: Displays detailed IPv4 VRRP group information. If you do not specify this keyword, the command displays brief IPv4 VRRP group information.

Usage guidelines

- If no interface or VRRP group is specified, this command displays the states of all IPv4 VRRP groups.
- If only an interface is specified, this command displays the states of all IPv4 VRRP groups on the specified interface.
- If both an interface and an IPv4 VRRP group are specified, this command displays the states of the specified IPv4 VRRP group on the specified interface.

Examples

```
# Display brief information about all IPv4 VRRP groups on the device when VRRP operates in standard mode.
```

```
<Sysname> display vrrp
```

```
IPv4 Virtual Router Information:
```

```
Running Mode      : Standard
```

```
Total number of virtual routers : 1
```

```
Interface          VRID  State      Running Adver  Auth  Virtual
```


| | | | Pri | Timer | Type | IP |
|-------|---|--------|-----|-------|--------|---------|
| Vlan1 | 1 | Master | 150 | 100 | Simple | 1.1.1.1 |

Table 31 Command output (in standard mode)

| Field | Description |
|---------------------------------|--|
| Running Mode | VRRP operating mode (standard mode). |
| Total number of virtual routers | Total number of VRRP groups. |
| Interface | Interface where the VRRP group is configured. |
| VRID | Virtual router ID (VRRP group number). |
| State | Status of the router in the VRRP group: <ul style="list-style-type: none"> • Master. • Backup. • Initialize. • Inactive. |
| Running Pri | Current priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes. |
| Adver Timer | VRRP advertisement sending interval in centiseconds. |
| Auth Type | Authentication type: <ul style="list-style-type: none"> • None—No authentication. • Simple—Simple text authentication. • MD5—MD5 authentication. |
| Virtual IP | Virtual IP address of the VRRP group. |

Display detailed information about all IPv4 VRRP groups on the device when VRRP operates in standard mode.

```
<Sysname> display vrrp verbose
IPv4 Virtual Router Information:
Running Mode      : Standard
Total number of virtual routers : 2
  Interface Vlan-interface2
    VRID          : 1                Adver Timer   : 100
    Admin Status  : Up                State         : Master
    Config Pri    : 150               Running Pri   : 150
    Preempt Mode  : Yes               Delay Time    : 5
    Auth Type     : Simple            Key           : *****
    Virtual IP    : 1.1.1.1
    Virtual MAC   : 0000-5e00-0101
    Master IP     : 1.1.1.2
VRRP Track Information:
  Track Object    : 1                State : Positive  Pri Reduced : 50
  Interface Vlan-interface2
    VRID          : 11               Adver Timer   : 100
    Admin Status  : Up                State         : Backup
```

```

Config Pri      : 80                      Running Pri    : 80
Preempt Mode   : Yes                      Delay Time    : 0
Become Master  : 2370ms left
Auth Type      : None
Virtual IP     : 1.1.1.11
Virtual MAC    : 0000-5e00-010b
Master IP      : 1.1.1.12

```

Table 32 Command output (in standard mode)

| Field | Description |
|---------------------------------|--|
| Running Mode | VRRP operating mode (standard mode). |
| Total number of virtual routers | Total number of VRRP groups. |
| Interface | Interface where the VRRP group is configured. |
| VRID | Virtual router ID (VRRP group number). |
| Adver Timer | VRRP advertisement sending interval in centiseconds. |
| Admin Status | Administrative status: up or down. |
| State | Status of the router in the VRRP group: <ul style="list-style-type: none"> • Master. • Backup. • Initialize. • Inactive. |
| Config Pri | Configured priority of the router, which is configured through the vrrp vrid priority command. |
| Running Pri | Current priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes. |
| Preempt Mode | Preemptive mode: <ul style="list-style-type: none"> • Yes. • No. |
| Delay Time | Preemption delay time in centiseconds. |
| Become Master | Time, in milliseconds, that a backup router has to wait before it becomes the master. |
| Auth Type | Authentication type: <ul style="list-style-type: none"> • None—No authentication. • Simple—Simple text authentication. • MD5—MD5 authentication. |
| Key | Authentication key, which is not displayed if no authentication is required. |
| Virtual IP | Virtual IP address of the VRRP group. |
| Virtual MAC | Virtual MAC address of the VRRP group's virtual IP address, which is displayed when the router is the master. |
| Master IP | Primary IP address of the interface where the master resides. |
| VRRP Track Information | Track entry information. This field is displayed only after you have configured the vrrp vrid track command. |

| Field | Description |
|--------------|---|
| Track Object | Track entry which is associated with the VRRP group. |
| State | Track entry state: <ul style="list-style-type: none"> Negative. Positive. NotReady. |
| Pri Reduced | Value by which the priority decreases when the status of the associated track entry becomes negative. |
| Switchover | Switchover mode. When the status of the associated track entry becomes negative, the backup immediately becomes the master. |

Display brief information about all IPv4 VRRP groups on the device when VRRP operates in load balancing mode.

```
<Sysname> display vrrp
```

```
IPv4 Virtual Router Information:
```

```
Running Mode      : Load Balance
```

```
Total number of virtual routers : 1
```

| Interface | VRID | State | Running Address Pri | Active |
|-----------|------|--------|------------------------|--------|
| Vlan1 | 1 | Master | 150 1.1.1.1 | Local |
| ----- | VF 1 | Active | 255 000f-e2ff-0011 | Local |

Table 33 Command output (in load balancing mode)

| Field | Description |
|---------------------------------|---|
| Running Mode | VRRP operating mode (load balancing mode). |
| Total number of virtual routers | Total number of VRRP groups. |
| Interface | Interface where the VRRP group is configured. |
| VRID | Virtual router ID (VRRP group number) or virtual forwarder (VF) ID. |
| State | <ul style="list-style-type: none"> For a VRRP group (when the VRID is a virtual router ID), this field indicates the state of the router in the VRRP group, including Master, Backup, Initialize, and Inactive. For a VF (when the VRID is a VF ID), this field indicates the state of the VF in the VRRP group, including Active, Listening, and Initialize. |
| Running Pri | <ul style="list-style-type: none"> For a VRRP group (when the VRID is a virtual router ID), this field indicates the running priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes. For a VF (when the VRID is a VF ID), this field indicates the running priority of the VF. When a track entry is associated with a VF, the priority of the VF changes if the state of the monitored track entry changes. |
| Address | <ul style="list-style-type: none"> For a VRRP group (when the VRID is a virtual router ID), this field indicates the virtual IP address of the VRRP group. For a VF (when the VRID is a VF ID), this field indicates the virtual MAC address of the VF. |

| Field | Description |
|--------|---|
| Active | <ul style="list-style-type: none"> For a VRRP group (when the VRID is a virtual router ID), this field indicates the IP address of the interface where the master resides. If the current router is the master, local is displayed. For a VF (when the VRID is a VF ID), this field indicates the IP address of the interface where the active virtual forwarder (AVF) resides. If the current VF is the AVF, local is displayed. |

Display detailed information about all IPv4 VRRP groups on the device when VRRP operates in load balancing mode.

```
<Sysname> display vrrp verbose
```

```
IPv4 Virtual Router Information:
```

```
Running Mode      : Load Balance
```

```
Total number of virtual routers : 2
```

```
Interface Vlan-interface
```

```
VRID              : 1                      Adver Timer   : 100
Admin Status      : Up                      State         : Master
Config Pri        : 150                     Running Pri    : 150
Preempt Mode      : Yes                     Delay Time    : 5
```

```
Auth Type         : None
```

```
Virtual IP        : 10.1.1.1
                  : 10.1.1.2
                  : 10.1.1.3
```

```
Member IP List   : 10.1.1.10 (Local, Master)
                  : 10.1.1.20 (Backup)
```

```
VRRP Track Information:
```

```
Track Object     : 1                      State : Positive   Pri Reduced : 50
```

```
Forwarder Information: 2 Forwarders 1 Active
```

```
Config Weight    : 255
```

```
Running Weight   : 255
```

```
Forwarder 01
```

```
State            : Active
Virtual MAC       : 000f-e2ff-0011 (Owner)
Owner ID         : 0000-5e01-1101
Priority          : 255
Active           : local
```

```
Forwarder 02
```

```
State            : Listening
Virtual MAC       : 000f-e2ff-0012 (Learnt)
Owner ID         : 0000-5e01-1103
Priority          : 127
Active           : 10.1.1.20
```

```
Forwarder Weight Track Information:
```

```
Track Object     : 1                      State : Positive   Weight Reduced : 250
```

```
Interface Vlan-interface2
```

```
VRID              : 11                     Adver Timer   : 100
Admin Status      : Up                      State         : Backup
Config Pri        : 80                      Running Pri    : 80
```

```

Preempt Mode      : Yes                Delay Time       : 0
Become Master    : 2370ms left
Auth Type        : None
Virtual IP       : 10.1.1.11
                  10.1.1.12
                  10.1.1.13
Member IP List   : 10.1.1.10 (Local, Backup)
                  10.1.1.15 (Master)
Forwarder Information: 2 Forwarders 1 Active
Config Weight    : 255
Running Weight   : 255
Forwarder 01
State            : Active
Virtual MAC      : 000f-e2ff-40b1 (Learnt)
Owner ID         : 0000-5e01-1103
Priority         : 127
Active           : 10.1.1.15
Forwarder 02
State            : Listening
Virtual MAC      : 000f-e2ff-40b2 (Owner)
Owner ID         : 0000-5e01-1101
Priority         : 255
Active           : local

```

Table 34 Command output (in load balancing mode)

| Field | Description |
|---------------------------------|---|
| Running Mode | VRRP operating mode (load balancing mode). |
| Total number of virtual routers | Total number of VRRP groups. |
| Interface | Interface where the VRRP group is configured. |
| VRID | Virtual router ID (VRRP group number). |
| Adver Timer | VRRP advertisement sending interval in centiseconds. |
| Admin Status | Administrative status: up or down. |
| State | Status of the router in the VRRP group: <ul style="list-style-type: none"> • Master. • Backup. • Initialize. • Inactive. |
| Config Pri | Configured priority of the router, which is configured by using the vrrp vrid priority command. |
| Running Pri | Current priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes. |
| Preempt Mode | Preemptive mode: <ul style="list-style-type: none"> • Yes. • No. |

| Field | Description |
|--|--|
| Delay Time | Preemption delay time in centiseconds. |
| Become Master | Time, in milliseconds, that a backup router has to wait before it becomes the master. |
| Auth Type | Authentication type: <ul style="list-style-type: none"> • None—No authentication. • Simple—Simple text authentication. • MD5—MD5 authentication. |
| Key | Authentication key, which is not displayed if no authentication is required. |
| Virtual IP | Virtual IP address list of the VRRP group. |
| Member IP List | IP addresses of the member devices in the VRRP group: <ul style="list-style-type: none"> • Local—IP address of the local router. • Master—IP address of the master. • Backup—IP address of the backup. |
| VRRP Track Information | Track entry which is associated with the VRRP group. This field is displayed only after you have configured the vrrp vrid track command. |
| Track Object | Track entry to be monitored. |
| State | Track entry state: <ul style="list-style-type: none"> • Negative. • Positive. • NotReady. |
| Pri Reduced | Value by which the priority decreases when the status of the associated track entry becomes negative. This field is displayed only after you have configured vrrp vrid track command. |
| Switchover | Switchover mode. When the status of the associated track entry becomes negative, the backup immediately becomes the master. |
| Forwarder Information: 2 Forwarders 1 Active | VF information: Two VFs exist, and one is the AVF. |
| Config Weight | Configured weight of the VF: 255. |
| Running Weight | Current weight of the VF. When a track entry is associated with the VFs of a VRRP group, the VFs' weights change when the track entry's status changes. |
| Forwarder 01 | Information about VF 01. |
| State | VF state: <ul style="list-style-type: none"> • Active. • Listening. • Initialize. |
| Virtual MAC | Virtual MAC address of the VF. |
| Owner ID | Real MAC address of the VF owner. |
| Priority | VF priority in the range of 1 to 255. |
| Active | IP address of the interface where the AVF resides. If the current VF is the AVF, local is displayed. |

| Field | Description |
|--------------------------------------|--|
| Forwarder Weight Track Configuration | VF weight Track configuration. The field is displayed only after you have configured the vrrp vrid weight track command. |
| Track Object | Track entry which is associated with the VFs. The field is displayed only after you have configured the vrrp vrid weight track command. |
| State | Track entry state: <ul style="list-style-type: none"> Negative. Positive. NotReady. |
| Weight Reduced | Value by which the weights of the VFs decrease when the state of the associated track entry changes to negative. The field is displayed only after you configure the vrrp vrid weight track command. |

display vrrp statistics

Use **display vrrp statistics** to display statistics for IPv4 VRRP groups.

Syntax

```
display vrrp statistics [ interface interface-type interface-number [ vrid virtual-router-id ] ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

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

vrid *virtual-router-id*: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

Usage guidelines

- If no interface or VRRP group is specified, this command displays statistics for all IPv4 VRRP groups.
- If only an interface is specified, this command displays statistics for all IPv4 VRRP groups on the specified interface.
- If both an interface and an IPv4 VRRP group are specified, this command displays statistics for the specified IPv4 VRRP group on the specified interface.

You can use the **reset vrrp statistics** command to clear statistics for IPv4 VRRP groups.

Examples

Display statistics for all IPv4 VRRP groups when VRRP operates in standard mode.

```
<Sysname> display vrrp statistics
Interface          : Vlan-interface2
VRID                : 1
```

```

Checksum Errors          : 0          Version Errors          : 0
Invalid Pkts Rcvd      : 0          Unexpected Pkts Rcvd    : 0
IP TTL Errors          : 0          Advertisement Interval Errors : 0
Invalid Auth Type     : 0          Auth Failures          : 0
Packet Length Errors   : 0          Auth Type Mismatch     : 0
Become Master         : 1          Address List Errors     : 0
Adver Rcvd           : 0          Priority Zero Pkts Rcvd : 0
Adver Sent            : 807         Priority Zero Pkts Sent  : 0

```

Global statistics

```

Checksum Errors          : 0
Version Errors          : 0
VRID Errors             : 0

```

Display statistics for all IPv4 VRRP groups when VRRP operates in load balancing mode.

<Sysname> display vrrp statistics

```

Interface              : Vlan-interface2
VRID                   : 1
Checksum Errors        : 0          Version Errors          : 0
Invalid Pkts Rcvd     : 0          Unexpected Pkts Rcvd    : 0
IP TTL Errors          : 0          Advertisement Interval Errors : 0
Invalid Auth Type     : 0          Auth Failures          : 0
Packet Length Errors   : 0          Auth Type Mismatch     : 0
Become Master         : 39          Address List Errors     : 0
Become AVF            : 13          Packet Option Errors    : 0
Adver Rcvd            : 2562         Priority Zero Pkts Rcvd : 1
Adver Sent             : 16373        Priority Zero Pkts Sent  : 49
Request Rcvd          : 2          Reply Rcvd              : 10
Request Sent          : 12          Reply Sent               : 2
Release Rcvd          : 0          VF Priority Zero Pkts Rcvd : 1
Release Sent          : 0          VF Priority Zero Pkts Sent  : 11
Redirect Timer Expires : 1          Time-out Timer Expires   : 0

```

Global statistics

```

Checksum Errors          : 0
Version Errors          : 0
VRID Errors             : 0

```

Table 35 Command output (in standard mode)

| Field | Description |
|-------------------------------|---|
| Interface | Interface where the VRRP group is configured. |
| VRID | VRRP group number. |
| Checksum Errors | Number of packets with checksum errors. |
| Version Errors | Number of packets with version errors. |
| Invalid Pkts Rcvd | Number of received packets of invalid packet types. |
| Unexpected Pkts Rcvd | Number of received unexpected packets. |
| Advertisement Interval Errors | Number of packets with advertisement interval errors. |

| Field | Description |
|-------------------------|---|
| IP TTL Errors | Number of packets with TTL errors. |
| Auth Failures | Number of packets with authentication failures. |
| Invalid Auth Type | Number of packets with authentication failures because of invalid authentication types. |
| Auth Type Mismatch | Number of packets with authentication failures because of mismatching authentication types. |
| Packet Length Errors | Number of packets with VRRP packet length errors. |
| Address List Errors | Number of packets with virtual IP address list errors. |
| Become Master | Number of times that the router elected as the master. |
| Priority Zero Pkts Rcvd | Number of received advertisements with the router priority of 0. |
| Adver Rcvd | Number of received advertisements. |
| Priority Zero Pkts Sent | Number of sent advertisements with the router priority of 0. |
| Adver Sent | Number of sent advertisements. |
| Global statistics | Global statistics for all VRRP groups. |
| Checksum Errors | Total number of packets with checksum errors. |
| Version Errors | Total number of packets with version errors. |
| VRID Errors | Total number of packets with VRID errors. |

Table 36 Command output (in load balancing mode)

| Field | Description |
|-------------------------------|---|
| Interface | Interface where the VRRP group is configured. |
| VRID | VRRP group number. |
| Checksum Errors | Number of packets with checksum errors. |
| Version Errors | Number of packets with version errors. |
| Invalid Pkts Rcvd | Number of received packets of invalid packet types. |
| Unexpected Pkts Rcvd | Number of received unexpected packets. |
| Advertisement Interval Errors | Number of packets with advertisement interval errors. |
| IP TTL Errors | Number of packets with TTL errors. |
| Auth Failures | Number of packets with authentication failures. |
| Invalid Auth Type | Number of packets with authentication failures because of invalid authentication types. |
| Auth Type Mismatch | Number of packets with authentication failures because of mismatching authentication types. |
| Packet Length Errors | Number of packets with VRRP packet length errors. |
| Address List Errors | Number of packets with virtual IP address list errors. |
| Become Master | Number of times that the router elected as the master. |
| Redirect Timer Expires | Number of times that the redirect timer expired. |

| Field | Description |
|----------------------------|--|
| Become AVF | Number of times that the VF elected as the AVF. |
| Time-out Timer Expires | Number of times that the time-out timer expired. |
| Adver Rcvd | Number of received advertisements. |
| Request Rcvd | Number of received requests. |
| Adver Sent | Number of sent advertisements. |
| Request Sent | Number of sent requests. |
| Reply Rcvd | Number of received replies. |
| Release Rcvd | Number of received release packets. |
| Reply Sent | Number of sent replies. |
| Release Sent | Number of sent release packets. |
| Priority Zero Pkts Rcvd | Number of received advertisements with the router priority of 0. |
| VF Priority Zero Pkts Rcvd | Number of received advertisements with the VF priority of 0. |
| Priority Zero Pkts Sent | Number of sent advertisements with the router priority of 0. |
| VF Priority Zero Pkts Sent | Number of sent advertisements with the VF priority of 0. |
| Packet Option Errors | Number of packet option errors. |
| Global statistics | Global statistics for all IPv4 VRRP groups. |
| Checksum Errors | Total number of packets with checksum errors. |
| Version Errors | Total number of packets with version errors. |
| VRID Errors | Total number of packets with VRID errors. |

Related commands

reset vrrp statistics

reset vrrp statistics

Use **reset vrrp statistics** to clear statistics for IPv4 VRRP groups.

Syntax

reset vrrp statistics [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

Views

User view

Predefined user roles

network-admin

Parameters

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

vrid *virtual-router-id*: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

Usage guidelines

- If no interface or VRRP group is specified, this command clears statistics for all IPv4 VRRP groups.

- If only an interface is specified, this command clears statistics for all IPv4 VRRP groups on the specified interface.
- If both an interface and an IPv4 VRRP group are specified, this command clears statistics for the specified IPv4 VRRP group on the specified interface.

Examples

```
# Clear statistics for all IPv4 VRRP groups on all interfaces.
<Sysname> reset vrrp statistics
```

Related commands

display vrrp statistics

snmp-agent trap enable vrrp

Use **snmp-agent trap enable vrrp** to enable SNMP notifications for VRRP globally.

Use **undo snmp-agent trap enable vrrp** to disable SNMP notifications for VRRP globally.

Syntax

```
snmp-agent trap enable vrrp [ auth-failure | new-master ]
undo snmp-agent trap enable vrrp [ auth-failure | new-master ]
```

Default

SNMP notifications for VRRP are enabled.

Views

System view

Predefined user roles

network-admin

Parameters

auth-failure: Generates notifications as defined in RFC 2787 when the device in a VRRP group receives a VRRP advertisement with the authentication type or key not matching the local configuration.

new-master: Generates notifications as defined in RFC 2787 when the state of a device in a VRRP group changes from Initialize or Backup to Master.

Usage guidelines

When the notification function is enabled, the device can send notifications to the destination host. To specify the notification type (inform or trap) and target host, use the **snmp-agent target-host** command.

Examples

```
# Generate notifications as defined in RFC 2787 when the device in a VRRP group receives a VRRP
advertisement with the authentication type or key not matching the local configuration.
<Sysname> system-view
[Sysname] snmp-agent trap enable vrrp auth-failure
```

vrrp check-ttl enable

Use **vrrp check-ttl enable** to enable TTL check for IPv4 VRRP packets.

Use **undo vrrp check-ttl enable** to disable TTL check for IPv4 VRRP packets.

Syntax

```
vrrp check-ttl enable  
undo vrrp check-ttl enable
```

Default

TTL check for IPv4 VRRP packets is enabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

The master in an IPv4 VRRP group periodically sends VRRP advertisements to declare its presence. The VRRP advertisements are multicast in the local subnet and cannot be forwarded by routers, so the TTL value is not changed. When the master sends VRRP advertisements, it sets the TTL value to 255. If you enable TTL check, the backups drop the VRRP advertisements with TTL other than 255, preventing attacks from other subnets.

Devices from different vendors might implement VRRP differently. When the device is interoperating with devices of other vendors, TTL check on VRRP packets might result in unexpected dropping of packets. In this scenario, use the **undo vrrp check-ttl enable** command to disable TTL check on VRRP packets.

Examples

```
# Disable TTL check for IPv4 VRRP packets.  
<Sysname> system-view  
[Sysname] interface vlan-interface 2  
[Sysname-Vlan-interface2] undo vrrp check-ttl enable
```

vrrp dscp

Use **vrrp dscp** to configure a DSCP value for VRRP packets.

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

Syntax

```
vrrp dscp dscp-value  
undo vrrp dscp
```

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value for VRRP packets, in the range of 0 to 63. The default is 48.

Usage guidelines

The DSCP value identifies the packet priority during transmission. A greater DSCP value means a higher packet priority.

Examples

```
# Configure the DSCP value for VRRP packets as 30.
<Sysname> system-view
[Sysname] vrrp dscp 30
```

vrrp mode

Use **vrrp mode** to specify the operating mode for IPv4 VRRP.

Use **undo vrrp mode** to restore the default.

Syntax

```
vrrp mode load-balance [ version-8 ]
undo vrrp mode
```

Default

IPv4 VRRP operates in standard mode.

Views

System view

Predefined user roles

network-admin

Parameters

load-balance: Specifies the load balancing mode.

version-8: Specifies the version carried in VRRP packets as 8.

Usage guidelines

After you create IPv4 VRRP groups on the router, you can specify their operating mode by using this command. All IPv4 VRRP groups on the router operate in the specified mode.

The **version-8** keyword takes effect only when the version of IPv4 VRRP configured on the interface is VRRPv2. The **version-8** keyword is required in the following conditions:

- A router running Comware V5 software or software with version earlier than Comware V7 exists in the VRRP group.
To display the software version, use the **display version** command.
- All routers in the IPv4 VRRP group are operating in load balancing mode.
- All routers in the IPv4 VRRP group are configured with the version of VRRPv2.

Examples

```
# Specify the load balancing mode for IPv4 VRRP.
<Sysname> system-view
[Sysname] vrrp mode load-balance
```

Related commands

display vrrp

vrrp version

Use **vrrp version** to specify the version of IPv4 VRRP on an interface.

Use **undo vrrp version** to restore the default.

Syntax

vrrp version *version-number*

undo vrrp version

Default

VRRPv3 is used.

Views

Interface view

Predefined user roles

network-admin

Parameters

version-number: Specifies a VRRP version. The version number is 2 or 3, where 2 indicates VRRPv2 (described in RFC 3768), and 3 indicates VRRPv3 (described in RFC 5798).

Usage guidelines

The version of VRRP on all routers in an IPv4 VRRP group must be the same.

Examples

```
# Specify VRRPv2 to run on VLAN-interface 10.
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] vrrp version 2
```

vrrp vrid

Use **vrrp vrid** to create an IPv4 VRRP group and assign a virtual IP address to the IPv4 VRRP group or to assign a virtual IP address to an existing IPv4 VRRP group.

Use **undo vrrp vrid** to remove all configurations of an existing IPv4 VRRP group or to remove a virtual IP address from an existing IPv4 VRRP group.

Syntax

vrrp vrid *virtual-router-id* **virtual-ip** *virtual-address*

undo vrrp vrid *virtual-router-id* [**virtual-ip** [*virtual-address*]]

Default

No IPv4 VRRP group is created.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

virtual-ip *virtual-address*: Specifies a virtual IP address, which cannot be an all-zero address (0.0.0.0); a broadcast address (255.255.255.255); a loopback address; an IP address of other than Class A, Class B, and Class C; or an invalid IP address (for example, 0.0.0.1). If you do not specify this option, the **undo vrrp vrid** command removes all virtual IP addresses from the existing IPv4 VRRP group.

Usage guidelines

You can assign up to 16 virtual IP addresses to an IPv4 VRRP group.

If you create an IPv4 VRRP group but do not assign any virtual IP address to it, the VRRP group stays in inactive state and does not function.

The virtual IP address of an IPv4 VRRP group and the downlink interface IP address of the VRRP group must be in the same subnet. Otherwise, the hosts in the subnet might fail to access external networks.

In load balancing mode, the virtual IP address of an IPv4 VRRP group cannot be the same as the IP address of any interface in the VRRP group. Otherwise, the load balancing mode cannot operate.

Examples

```
# Create IPv4 VRRP group 1 and assign virtual IP address 10.10.10.10 to the VRRP group. Then assign virtual IP address 10.10.10.11 to the VRRP group.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.10.10.10
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.10.10.11
```

Related commands

display vrrp

vrrp vrid authentication-mode

Use **vrrp vrid authentication-mode** to configure the authentication mode and the authentication key for an IPv4 VRRP group to send and receive VRRP packets.

Use **undo vrrp vrid authentication-mode** to restore the default.

Syntax

```
vrrp vrid virtual-router-id authentication-mode { md5 | simple } { cipher | plain } key
```

```
undo vrrp vrid virtual-router-id authentication-mode
```

Default

Authentication is disabled when a VRRP group sends and receives VRRP packets.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

md5: Specifies the MD5 authentication mode.

simple: Specifies the simple authentication mode.

cipher: Sets a ciphertext authentication key.

plain: Sets a plaintext authentication key.

key: Sets the authentication key. This argument is case-sensitive. It must be a ciphertext string of 1 to 41 characters if the **cipher** keyword is specified or a plaintext string of 1 to 8 characters if the **plain** keyword is specified.

Usage guidelines

To avoid attacks from unauthorized users, VRRP member routers add authentication keys in VRRP packets to authenticate one another. VRRP provides the following authentication modes:

- **simple**—Simple text authentication.
The sender fills an authentication key into the VRRP packet, and the receiver compares the received authentication key with its local authentication key. If the two authentication keys are the same, the received VRRP packet is legitimate. Otherwise, the received packet is illegitimate.
- **md5**—MD5 authentication.
The sender computes a digest for the packet to be sent by using the authentication key and MD5 algorithm, and it saves the result in the authentication header. The receiver performs the same operation by using the authentication key and MD5 algorithm, and it compares the result with the content in the authentication header. If the results are the same, the received VRRP packet is legitimate. Otherwise, the received packet is illegitimate.

The MD5 authentication is more secure than the simple text authentication, but it costs more resources. For security purposes, all keys, including keys configured in plain text, are saved in cipher text.

! IMPORTANT:

- You can configure different authentication modes and authentication keys for the VRRP groups on an interface. However, members of the same VRRP group must use the same authentication mode and authentication key.
 - For VRRPv3, this command does not take effect.
-

Examples

```
# Set the authentication mode to simple and the authentication key to Sysname for VRRP group 1 on VLAN-interface 2.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 authentication-mode simple plain Sysname
```

Related commands

- **display vrrp**
- **vrrp version**

vrrp vrid preempt-mode

Use **vrrp vrid preempt-mode** to enable the preemptive mode for the device in an IPv4 VRRP group and configure the preemption delay.

Use **undo vrrp vrid preempt-mode** to disable the preemptive mode for the device in an IPv4 VRRP group.

Use **undo vrrp vrid preempt-mode delay** to restore the default preemption delay.

Syntax

vrrp vrid *virtual-router-id* **preempt-mode** [**delay** *delay-value*]

undo vrrp vrid *virtual-router-id* **preempt-mode** [**delay**]

Default

The device operates in preemptive mode and the preemption delay is 0 centiseconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

delay *delay-value*: Specifies a preemption delay time in the range of 0 to 180000 in centiseconds. The default setting is 0 centiseconds.

Usage guidelines

In non-preemptive mode, when a device in the IPv4 VRRP group becomes the master, it acts as the master as long as it operates correctly, even if a backup is assigned a higher priority later. The non-preemptive mode helps avoid frequent switchover between the master and backups.

In preemptive mode, a backup takes over as the master and sends VRRP advertisements when it detects that it has a higher priority than the master. The previous master then becomes a backup. This mechanism makes sure the master is always the device with the highest priority.

To avoid frequent state changes among members in a VRRP group and to provide the backups enough time to collect information (such as routing information), a backup does not immediately become the master after it receives an advertisement with lower priority than the local priority. Instead, it waits for a period of time before taking over as the master.

Examples

```
# Enable the preemptive mode for VLAN-interface 2, and set the preemption delay time to 500 centiseconds.
```

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

```
[Sysname] interface vlan-interface 2
```

```
[Sysname-Vlan-interface2] vrrp vrid 1 preempt-mode delay 500
```

Related commands

display vrrp

vrrp vrid priority

Use **vrrp vrid priority** to configure the priority of the device in an IPv4 VRRP group.

Use **undo vrrp vrid priority** to restore the default.

Syntax

vrpp vrid *virtual-router-id* **priority** *priority-value*

undo vrpp vrid *virtual-router-id* **priority**

Default

The priority of a device in an IPv4 VRRP group is 100.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

priority-value: Specifies a priority value in the range of 1 to 254. A higher number indicates a higher priority.

Usage guidelines

VRRP determines the role (master or backup) of each device in a VRRP group by priority. A device with a higher priority is more likely to become the master.

VRRP priority is in the range of 0 to 255, and a greater number represents a higher priority. Priorities 1 to 254 are configurable. Priority 0 is reserved for special uses, and priority 255 is for the IP address owner. The device acting as the IP address owner in a VRRP group always has a running priority of 255 and acts as the master as long as it works correctly.

Examples

```
# Configure the priority of the switch in VRRP group 1 on VLAN-interface 2 to 150.
```

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

```
[Sysname] interface vlan-interface 2
```

```
[Sysname-Vlan-interface2] vrpp vrid 1 priority 150
```

Related commands

- **display vrpp**
- **vrpp vrid track**

vrpp vrid shutdown

Use **vrpp vrid shutdown** to disable an IPv4 VRRP group.

Use **undo vrpp vrid shutdown** to restore the default.

Syntax

vrpp vrid *virtual-router-id* **shutdown**

undo vrpp vrid *virtual-router-id* **shutdown**

Default

An IPv4 VRRP group is enabled.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

Usage guidelines

You can use this command to temporarily disable an IPv4 VRRP group. After this command is configured, the VRRP group stays in initialized state, and its configurations remain unchanged. You can change its configuration and your changes take effect when you enable the VRRP group again.

Examples

```
# Disable IPv4 VRRP group 1.
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 shutdown
```

vrrp vrid source-interface

Use **vrrp vrid source-interface** to specify the source interface for an IPv4 VRRP group. This interface, instead of the interface where the VRRP group resides, sends and receives VRRP packets.

Use **undo vrrp source-interface** to cancel the specified source interface.

Syntax

vrrp vrid *virtual-router-id* **source-interface** *interface-type interface-number*

undo vrrp vrid *virtual-router-id* **source-interface**

Default

No source interface is specified for a VRRP group. The interface where the VRRP group resides sends and receives VRRP packets.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

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

Usage guidelines

If VRRP group members cannot exchange VRRP packets through the interfaces where the VRRP group resides, you can use this command to enable VRRP packet exchange among VRRP group members through the specified source interfaces.

Examples

```
# Specify VLAN-interface 20 as the source interface for VRRP packet exchange in IPv4 VRRP group 10.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] vrrp vrid 10 source-interface vlan-interface 20
```

vrrp vrid timer advertise

Use **vrrp vrid timer advertise** to configure the interval at which the master in an IPv4 VRRP group sends VRRP advertisements.

Use **undo vrrp vrid timer advertise** to restore the default.

Syntax

vrrp vrid *virtual-router-id* **timer advertise** *adver-interval*

undo vrrp vrid *virtual-router-id* **timer advertise**

Default

The master in an IPv4 VRRP group sends VRRP advertisements at an interval of 100 centiseconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group by its virtual router ID in the range of 1 to 255.

adver-interval: Specifies an interval for the master in the specified IPv4 VRRP group to send VRRP advertisements. The value range for this argument is 10 to 4095 centiseconds. For VRRPv2, the value of the *adver-interval* argument can only be a multiple of 100. For example, if you configure values in the range of 10 to 100, 101 to 200, and 4001 to 4095, the actual values are 100, 200, and 4100, respectively. For VRRPv3, the value of the *adver-interval* argument that you configured takes effect.

Usage guidelines

The master in an IPv4 VRRP group periodically sends VRRP advertisements to declare its presence. You can use this command to configure the interval at which the master sends VRRP advertisements.

HP recommends that you set the VRRP advertisement interval to be greater than 100 centiseconds to maintain system stability.

In VRRPv2, all routers in an IPv4 VRRP group must have the same interval for sending VRRP advertisements.

In VRRPv3, the routers in an IPv4 VRRP group can have different intervals for sending VRRP advertisements. The master in the VRRP group sends VRRP advertisements at the specified interval and carries the interval attribute in the advertisements. After a backup receives the advertisement, it records the interval in the advertisement. If the backup does not receive a new VRRP advertisement from the master when the timer ($3 \times \text{recorded interval} + \text{Skew_Time}$) expires, it regards the master as failed and takes over as the master.

Large network traffic might disable a backup from receiving VRRP advertisements from the master within the specified time and trigger an unexpected master switchover. To solve this problem, you can use this command to configure a larger interval.

Examples

```
# Configure the master in IPv4 VRRP group 1 to send VRRP advertisements at an interval of 500
centiseconds.
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 timer advertise 500
```

Related commands

display vrrp

vrrp vrid track

Use **vrrp vrid track** to associate a VRRP group with a track entry and control master switchover or AVF switchover in the VRRP group in response to changes (such as uplink state changes) detected by the track entry.

Use **undo vrrp vrid track** to remove the association between a VRRP group and a track entry. If no track entry is specified, the association between the VRRP group and any track entry is removed.

Syntax

vrrp vrid *virtual-router-id* **track** *track-entry-number* { **forwarder-switchover member-ip** *ip-address* | **priority reduced** [*priority-reduced*] | **switchover** | **weight reduced** [*weight-reduced*] }

undo vrrp vrid *virtual-router-id* **track** [*track-entry-number* [**forwarder-switchover** | **priority reduced** | **switchover** | **weight reduced**]]

Default

A VRRP group is not associated with any track entry.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv4 VRRP group number in the range of 1 to 255.

track-entry-number: Specifies a track entry. The *track-entry-number* argument is in the range of 1 to 1024.

forwarder-switchover member-ip ip-address: Enables the LVF on the router to take over the role of the AVF at the specified IP address immediately after the specified track entry changes to the negative state. You can use the **display vrrp verbose** command to view the IP addresses of VFs.

priority reduced *priority-reduced*: Reduces the priority of the router in the VRRP group by a specific value when the state of the specified track entry changes to negative. The *priority-reduced* argument is in the range of 1 to 255, and the default is 10.

switchover: Enables the router in backup state to take over as the master immediately after the specified track entry changes to the negative state.

weight reduced *priority-reduced*: Reduces the weight of all VFs on the router in the VRRP group by a specific value when the state of the specified track entry changes to negative. The *weight-reduced* argument is in the range of 1 to 255, and the default is 30.

Usage guidelines

When the associated track entry changes to the negative state, one of the following conditions occurs, depending on your configuration:

- The priority of the router in the VRRP group decreases by a specific value.
- The weight of VFs decreases by a specific value.
- The router immediately takes over as the master if it is a backup.
- The LVF on the router takes over the role of the AVF at the specified IP address immediately.

Before executing this command, create a VRRP group on the interface and assign a virtual IP address to it.

The **forwarder-switchover member-ip** *ip-address* or **weight reduced** *weight-reduced* option takes effect only when the IPv4 VRRP group is operating in load balancing mode.

If the **priority reduced** keyword is specified but the *priority-reduced* argument is not specified, the priority of the router in the VRRP group decreases by 10 when the track entry changes to **negative**.

If the **weight reduced** keyword is specified but the *weight-reduced* argument is not specified, the weight of the VFs on the router in the VRRP group decreases by 30 when the track entry changes to **negative**.

The weight of a VF is 255, and its lower limit of failure is 10.

When the weight of a VF owner is higher than or equal to the lower limit of failure, its priority is always 255 and does not change with the weight. To guarantee that an LVF can take over the VF owner as the AVF when the upstream link of the VF owner fails, the reduced weight for the VF owner must be higher than 245 so the weight of the VF owner can drop below the lower limit of failure.

When the track entry changes from Negative to Positive or NotReady, the router automatically restores its priority or VF weight. The failed master router becomes the master again, or the failed AVF becomes active again.

! IMPORTANT:

- The **vrrp vrid track priority reduced** or **vrrp vrid track switchover** command cannot take effect on an IP address owner. If you have configured the command on an IP address owner, the configuration takes effect after the router changes to be a non-IP address owner.
 - You can create a track entry with the **track** command before or after you associate it with a VRRP group. For more information about configuring track entries, see *High Availability Configuration Guide*.
-

Examples

```
# Associate VRRP group 1 on VLAN-interface 2 with track entry 1 and decrease the priority of the router in the VRRP group by 50 when the state of track entry 1 changes to negative.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 track 1 priority reduced 50
```

```
# Associate VRRP group 1 on VLAN-interface 2 with track entry 1 and enable the VF in listening state whose AVF is on the member device with the IP address of 10.1.1.3 to take over immediately after the specified track entry changes to the negative state.
```

```
[Sysname-Vlan-interface2] vrrp vrid 1 track 1 forwarder-switchover member-ip 10.1.1.3
```

```
# Associate VRRP group 1 on VLAN-interface 2 with track entry 1 and decrease the weight of all VFs on the router in the VRRP group by 50 when the state of track entry 1 changes to negative.
```

```
[Sysname-Vlan-interface2] vrrp vrid 1 track 1 weight reduced 50
```

Related commands

`display vrrp`

IPv6 VRRP commands

display vrrp ipv6

Use `display vrrp ipv6` to display the states of IPv6 VRRP groups.

Syntax

`display vrrp ipv6 [interface interface-type interface-number [vrid virtual-router-id]] [verbose]`

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

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

vrid *virtual-router-id*: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

verbose: Displays detailed IPv6 VRRP group information. If you do not specify this keyword, the command displays brief IPv6 VRRP group information.

Usage guidelines

- If no interface or VRRP group is specified, this command displays the states of all IPv6 VRRP groups.
- If only an interface is specified, this command displays the states of all IPv6 VRRP groups on the specified interface.
- If both an interface and an IPv6 VRRP group are specified, this command displays the states of the specified IPv6 VRRP group on the specified interface.

Examples

Display brief information about all IPv6 VRRP groups on the device when VRRP operates in standard mode.

```
<Sysname> display vrrp ipv6
IPv6 Virtual Router Information:
Running Mode      : Standard
Total number of virtual routers : 1
Interface         VRID  State      Running Adver   Auth   Virtual
                  Pri   Timer     Type      IP
-----
Vlan1             1    Master     150      100    None   FE80::1
```

Table 37 Command output (in standard mode)

| Field | Description |
|--------------|--------------------------------------|
| Running Mode | VRRP operating mode (standard mode). |

| Field | Description |
|---------------------------------|---|
| Total number of virtual routers | Total number of VRRP groups. |
| Interface | Interface where the VRRP group is configured. |
| VRID | Virtual router ID (VRRP group number). |
| State | Status of the router in the VRRP group: <ul style="list-style-type: none"> • Master. • Backup. • Initialize. • Inactive. |
| Running Pri | Current priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes. |
| Adver Timer | VRRP advertisement sending interval in centiseconds. |
| Auth Type | Authentication type. Only none is available, which means no authentication is required. |
| Virtual IP | Virtual IP address of the VRRP group. |

Display detailed information about all IPv6 VRRP groups on the device when VRRP operates in standard mode.

```
<Sysname> display vrrp ipv6 verbose
```

```
IPv6 Virtual Router Information:
```

```
Running Mode      : Standard
```

```
Total number of virtual routers : 2
```

```
Interface Vlan-interface2
```

```
VRID           : 1                Adver Timer   : 100
Admin Status   : Up                State          : Master
Config Pri     : 150               Running Pri    : 150
Preempt Mode   : Yes               Delay Time     : 10
Auth Type      : None
Virtual IP     : FE80::1
Virtual MAC    : 0000-5e00-0201
Master IP      : FE80::2
```

```
VRRP Track Information:
```

```
Track Object    : 1                State : Positive  Pri Reduced : 50
```

```
Interface Vlan-interface2
```

```
VRID           : 11               Adver Timer   : 100
Admin Status   : Up                State          : Backup
Config Pri     : 80                Running Pri    : 80
Preempt Mode   : Yes               Delay Time     : 0
Become Master  : 2450ms left
Auth Type      : None
Virtual IP     : FE80::11
Virtual MAC    : 0000-5e00-020b
Master IP      : FE80::12
```


Table 38 Command output (in standard mode)

| Field | Description |
|---------------------------------|---|
| Running Mode | VRRP operating mode (standard mode). |
| Total number of virtual routers | Total number of VRRP groups. |
| Interface | Interface where the VRRP group is configured. |
| VRID | Virtual router ID (VRRP group number). |
| Adver Timer | VRRP advertisement sending interval in centiseconds. |
| Admin Status | Administrative status: up or down. |
| State | Status of the router in the VRRP group: <ul style="list-style-type: none"> • Master. • Backup. • Initialize. • Inactive. |
| Config Pri | Configured priority of the router, which is configured through the vrrp ipv6 vrid priority command. |
| Running Pri | Current priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes. |
| Preempt Mode | Preemptive mode: <ul style="list-style-type: none"> • Yes. • No. |
| Delay Time | Preemption delay time in centiseconds. |
| Become Master | Time, in milliseconds, that a backup router has to wait before it becomes the master. |
| Auth Type | Authentication type. Only none is available, which means no authentication is required. |
| Virtual IP | Virtual IP address of the VRRP group. |
| Virtual MAC | Virtual MAC address of the VRRP group's virtual IP address, which is displayed when the router is the master. |
| Master IP | Link-local address of the interface where the master resides. |
| VRRP Track Information | Track entry information. This field is displayed only after you have configured the vrrp ipv6 vrid track command. |
| Track Object | Track entry which is associated with the VRRP group. |
| State | Track entry state: <ul style="list-style-type: none"> • Negative. • Positive. • NotReady. |
| Pri Reduced | Value by which the priority decreases when the status of the associated track entry becomes negative. |
| Switchover | Switchover mode. When the status of the associated track entry becomes negative, the backup immediately becomes the master. |

Display brief information about all IPv6 VRRP groups on the device when VRRP operates in load balancing mode.

```
<Sysname> display vrrp ipv6
IPv6 Virtual Router Information:
Running Mode      : Load Balance
Total number of virtual routers : 1
Interface        VRID  State      Running Address      Active
                  Pri
-----
Vlan1            1    Master    150    FE80::1    Local
-----
VF 1             1    Active    255    000f-e2ff-4011    Local
```

Table 39 Command output (in load balancing mode)

| Field | Description |
|---------------------------------|---|
| Running Mode | VRRP operating mode (load balancing mode). |
| Total number of virtual routers | Total number of VRRP groups. |
| Interface | Interface where the VRRP group is configured. |
| VRID | Virtual router ID (VRRP group number) or VF ID. |
| State | <ul style="list-style-type: none"> For a VRRP group (when the VRID is a virtual router ID), this field indicates the state of the router in the VRRP group, including Master, Backup, Initialize, and Inactive. For a VF (when the VRID is a VF ID), this field indicates the state of the VF in the VRRP group, including Active, Listening, and Initialize. |
| Running Pri | <ul style="list-style-type: none"> For a VRRP group (when the VRID is a virtual router ID), this field indicates the running priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes. For a VF (when the VRID is a VF ID), this field indicates the running priority of the VF. When a track entry is associated with a VF, the priority of the VF changes if the state of the monitored track entry changes. |
| Address | <ul style="list-style-type: none"> For a VRRP group (when the VRID is a virtual router ID), this field indicates the virtual IP address of the VRRP group. For a VF (when the VRID is a VF ID), this field indicates the virtual MAC address of the VF. |
| Active | <ul style="list-style-type: none"> For a VRRP group (when the VRID is a virtual router ID), this field indicates the link-local address of the interface where the master resides. If the current router is the master, local is displayed. For a VF (when the VRID is a VF ID), this field indicates the link-local address of the interface where the AVF resides. If the current VF is the AVF, local is displayed. |

Display detailed information about all IPv6 VRRP groups on the device when VRRP operates in load balancing mode.

```
<Sysname> display vrrp ipv6 verbose
IPv6 Virtual Router Information:
Running Mode      : Load Balance
Total number of virtual routers : 2
Interface Vlan-interface2
```

```

VRID          : 1                      Adver Timer   : 100
Admin Status  : Up                      State         : Master
Config Pri    : 150                     Running Pri   : 150
Preempt Mode  : Yes                     Delay Time    : 5
Auth Type     : None
Virtual IP    : FE80::10
Member IP List : FE80::3 (Local, Master)
                FE80::2 (Backup)

VRRP Track Information:
Track Object   : 1                      State : Positive   Pri Reduced : 50
Forwarder Information: 2 Forwarders 1 Active
Config Weight  : 255
Running Weight : 255
Forwarder 01
State          : Active
Virtual MAC    : 000f-e2ff-4011 (Owner)
Owner ID      : 0000-5e01-1101
Priority       : 255
Active        : local
Forwarder 02
State          : Listening
Virtual MAC    : 000f-e2ff-4012 (Learnt)
Owner ID      : 0000-5e01-1103
Priority       : 127
Active        : FE80::2
Forwarder Weight Track Information:
Track Object   : 1                      State : Positive   Weight Reduced : 250
Interface Vlan-interface2
VRID          : 11                      Adver Timer   : 100
Admin Status  : Up                      State         : Backup
Config Pri    : 80                     Running Pri   : 80
Preempt Mode  : Yes                     Delay Time    : 0
Become Master : 2450ms left
Auth Type     : None
Virtual IP    : FE80::11
Member IP List : FE80::3 (Local, Backup)
                FE80::2 (Master)

Forwarder Information: 2 Forwarders 1 Active
Config Weight  : 255
Running Weight : 255
Forwarder 01
State          : Active
Virtual MAC    : 000f-e2ff-40b1 (Learnt)
Owner ID      : 0000-5e01-1103
Priority       : 127
Active        : FE80::2
Forwarder 02
State          : Listening

```

```

Virtual MAC      : 000f-e2ff-40b2 (Owner)
Owner ID        : 0000-5e01-1101
Priority         : 255
Active          : local

```

Table 40 Command output (in load balancing mode)

| Field | Description |
|---------------------------------|--|
| Running Mode | VRRP operating mode (load balancing mode). |
| Total number of virtual routers | Total number of VRRP groups. |
| Interface | Interface where the VRRP group is configured. |
| VRID | Virtual router ID (VRRP group number) |
| Adver Timer | VRRP advertisement sending interval in centiseconds. |
| Admin Status | Administrative status: up or down. |
| State | Status of the router in the VRRP group: <ul style="list-style-type: none"> • Master. • Backup. • Initialize. • Inactive. |
| Config Pri | Configured priority of the router, which is configured through the vrrp ipv6 vrid priority command. |
| Running Pri | Current priority of the router. When a track entry is associated with a VRRP group on the router, the router's priority changes when the track entry's status changes. |
| Preempt Mode | Preemptive mode: <ul style="list-style-type: none"> • Yes. • No. |
| Delay Time | Preemption delay time in centiseconds. |
| Become Master | Time, in milliseconds, that a backup router has to wait before it becomes the master. |
| Auth Type | Authentication type. Only none is available, which means no authentication is required. |
| Virtual IP | Virtual IP address list of the VRRP group. |
| Member IP List | IP addresses of the member devices in the VRRP group: <ul style="list-style-type: none"> • Local—IP address of the local router. • Master—IP address of the master. • Backup—IP address of the backup. |
| VRRP Track Information | Track entry which is associated with the VRRP group. This field is displayed only after you have configured the vrrp ipv6 vrid track command. |
| Track Object | Track entry to be monitored. This field is displayed only after you have configured the vrrp ipv6 vrid track command. |

| Field | Description |
|---|---|
| State | Track entry state: <ul style="list-style-type: none"> Negative. Positive. NotReady. |
| Pri Reduced | Value by which the priority decreases when the status of the associated track entry becomes negative. This field is displayed only after you have configured vrrp ipv6 vrid track command. |
| Switchover | Switchover mode. When the status of the associated track entry becomes negative, the backup immediately becomes the master. |
| Forwarder Information: 2 Forwarders 1 Active | VF information: Two VFs exist and one is the AVF. |
| Config Weight | Configured weight of the VF: 255. |
| Running Weight | Current weight of the VF. When a track entry is associated with the VFs of a VRRP group, the VFs' weights change when the track entry's status changes. |
| Forwarder 01 | Information about VF 01. |
| State | VF state: <ul style="list-style-type: none"> Active. Listening. Initialize. |
| Virtual MAC | Virtual MAC address of the VF. |
| Owner ID | Real MAC address of the VF owner. |
| Priority | VF priority in the range of 1 to 255. |
| Active | Link-local address of the interface where the AVF resides. If the current VF is the AVF, local is displayed. |
| Forwarder Weight Track Configuration | VF weight Track configuration. The field is displayed only after you have configured the vrrp ipv6 vrid weight track command. |
| Track Object | Track entry which is associated with the VFs. The field is displayed only after you have configured the vrrp ipv6 vrid weight track command. |
| State | Track entry state: <ul style="list-style-type: none"> Negative. Positive. NotReady. |
| Weight Reduced | Value by which the weights of the VFs decrease when the state of the associated track entry changes to negative. The field is displayed only after you have configured the vrrp ipv6 vrid weight track command. |

display vrrp ipv6 statistics

Use **display vrrp ipv6 statistics** to display statistics for IPv6 VRRP groups.

Syntax

```
display vrrp ipv6 statistics [ interface interface-type interface-number [ vrid virtual-router-id ] ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

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

vrid *virtual-router-id*: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

Usage guidelines

- If no interface or VRRP group is specified, this command displays statistics for all IPv6 VRRP groups.
- If only an interface is specified, this command displays statistics for all IPv6 VRRP groups on the specified interface.
- If both an interface and an IPv6 VRRP group are specified, this command displays statistics for the specified IPv6 VRRP group on the specified interface.

You can use the **reset vrrp ipv6 statistics** command to clear statistics for IPv6 VRRP groups.

Examples

Display statistics for all IPv6 VRRP groups when VRRP operates in standard mode.

```
<Sysname> display vrrp ipv6 statistics
Interface                : Vlan-interface2
VRID                     : 1
Checksum Errors          : 0           Version Errors                : 0
Invalid Pkts Rcvd       : 0           Unexpected Pkts Rcvd          : 0
Hop Limit Errors        : 0           Advertisement Interval Errors : 0
Invalid Auth Type       : 0           Auth Failures                 : 0
Packet Length Errors    : 0           Auth Type Mismatch           : 0
Become Master           : 1           Address List Errors           : 0
Adver Rcvd              : 0           Priority Zero Pkts Rcvd       : 0
Adver Sent               : 425         Priority Zero Pkts Sent       : 0
```

Global statistics

```
Checksum Errors          : 0
Version Errors           : 0
VRID Errors              : 0
```

Display statistics for all IPv6 VRRP groups when VRRP operates in load balancing mode.

```
<Sysname> display vrrp ipv6 statistics
Interface                : Vlan-interface2
VRID                     : 1
```

```

Checksum Errors          : 0          Version Errors          : 0
Invalid Pkts Rcvd       : 0          Unexpected Pkts Rcvd    : 0
Hop Limit Errors        : 0          Advertisement Interval Errors : 0
Invalid Auth Type       : 0          Auth Failures          : 0
Packet Length Errors    : 0          Auth Type Mismatch     : 0
Become Master           : 39         Address List Errors     : 0
Become AVF              : 13         Packet Option Errors    : 0
Adver Rcvd              : 2562        Priority Zero Pkts Rcvd : 1
Adver Sent              : 16373       Priority Zero Pkts Sent : 49
Request Rcvd           : 2           Reply Rcvd              : 10
Request Sent           : 12          Reply Sent              : 2
Release Rcvd           : 0           VF Priority Zero Pkts Rcvd : 1
Release Sent           : 0           VF Priority Zero Pkts Sent : 11
Redirect Timer Expires  : 1           Time-out Timer Expires  : 0

Global statistics
Checksum Errors          : 0
Version Errors          : 0
VRID Errors             : 0

```

Table 41 Command output (in standard mode)

| Field | Description |
|-------------------------------|---|
| Interface | Interface where the VRRP group is configured. |
| VRID | VRRP group number. |
| Checksum Errors | Number of packets with checksum errors. |
| Version Errors | Number of packets with version errors. |
| Invalid Pkts Rcvd | Number of received packets of invalid packet types. |
| Unexpected Pkts Rcvd | Number of received unexpected packets. |
| Advertisement Interval Errors | Number of packets with advertisement interval errors. |
| Hop Limit Errors | Number of packets with hop limit errors. |
| Auth Failures | Number of packets with authentication failures. |
| Invalid Auth Type | Number of packets with authentication failures because of invalid authentication types. |
| Auth Type Mismatch | Number of packets with authentication failures because of mismatching authentication types. |
| Packet Length Errors | Number of packets with VRRP packet length errors. |
| Address List Errors | Number of packets with virtual IP address list errors. |
| Become Master | Number of times that the router elected as the master. |
| Priority Zero Pkts Rcvd | Number of received advertisements with the router priority of 0. |
| Adver Rcvd | Number of received advertisements. |
| Priority Zero Pkts Sent | Number of sent advertisements with the router priority of 0. |
| Adver Sent | Number of sent advertisements. |
| Global statistics | Global statistics for all IPv6 VRRP groups. |

| Field | Description |
|-----------------|---|
| Checksum Errors | Total number of packets with checksum errors. |
| Version Errors | Total number of packets with version errors. |
| VRID Errors | Total number of packets with VRID errors. |

Table 42 Command output (in load balancing mode)

| Field | Description |
|-------------------------------|---|
| Interface | Interface where the VRRP group is configured. |
| VRID | VRRP group number. |
| Checksum Errors | Number of packets with checksum errors. |
| Version Errors | Number of packets with version errors. |
| Invalid Pkts Rcvd | Number of received packets of invalid packet types. |
| Unexpected Pkts Rcvd | Number of received unexpected packets. |
| Advertisement Interval Errors | Number of packets with advertisement interval errors. |
| Hop Limit Errors | Number of packets with hop limit errors. |
| Auth Failures | Number of packets with authentication failures. |
| Invalid Auth Type | Number of packets with authentication failures because of invalid authentication types. |
| Auth Type Mismatch | Number of packets with authentication failures because of mismatching authentication types. |
| Packet Length Errors | Number of packets with VRRP packet length errors. |
| Address List Errors | Number of packets with virtual IP address list errors. |
| Become Master | Number of times that the router elected as the master. |
| Redirect Timer Expires | Number of times that the redirect timer expired. |
| Become AVF | Number of times that the VF elected as the AVF. |
| Time-out Timer Expires | Number of times that the time-out timer expired. |
| Adver Rcvd | Number of received advertisements. |
| Request Rcvd | Number of received requests. |
| Adver Sent | Number of sent advertisements. |
| Request Sent | Number of sent requests. |
| Reply Rcvd | Number of received replies. |
| Release Rcvd | Number of received release packets. |
| Reply Sent | Number of sent replies. |
| Release Sent | Number of sent release packets. |
| Priority Zero Pkts Rcvd | Number of received advertisements with the router priority of 0. |
| VF Priority Zero Pkts Rcvd | Number of received advertisements with the VF priority of 0. |
| Priority Zero Pkts Sent | Number of sent advertisements with the router priority of 0. |

| Field | Description |
|----------------------------|--|
| VF Priority Zero Pkts Sent | Number of sent advertisements with the VF priority of 0. |
| Packet Option Errors | Number of packet option errors. |
| Global statistics | Global statistics for all IPv6 VRRP groups. |
| Checksum Errors | Total number of packets with checksum errors. |
| Version Errors | Total number of packets with version errors. |
| VRID Errors | Total number of packets with VRID errors. |

Related commands

reset vrrp ipv6 statistics

reset vrrp ipv6 statistics

Use **reset vrrp ipv6 statistics** to clear statistics for IPv6 VRRP groups.

Syntax

reset vrrp ipv6 statistics [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

Views

User view

Predefined user roles

network-admin

Parameters

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

vrid *virtual-router-id*: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

Usage guidelines

- If no interface or VRRP group is specified, this command clears statistics for all IPv6 VRRP groups.
- If only an interface is specified, this command clears statistics for all IPv6 VRRP groups on the specified interface.
- If both an interface and an IPv6 VRRP group are specified, this command clears statistics for the specified IPv6 VRRP group on the specified interface.

Examples

```
# Clear statistics for all IPv6 VRRP groups on all interfaces.
```

```
<Sysname> reset vrrp ipv6 statistics
```

Related commands

display vrrp ipv6 statistics

vrrp ipv6 dscp

Use **vrrp ipv6 dscp** to configure a DSCP value for IPv6 VRRP packets.

Use **undo vrrp ipv6 dscp** to restore the default.

Syntax

```
vrrip ipv6 dscp dscp-value  
undo vrrip ipv6 dscp
```

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value for IPv6 VRRP packets, in the range of 0 to 63. The default is 56.

Usage guidelines

The DSCP value identifies the packet priority during transmission. A greater DSCP value means a higher packet priority.

Examples

```
# Configure the DSCP value for IPv6 VRRP packets as 30.  
<Sysname> system-view  
[Sysname] vrrip ipv6 dscp 30
```

vrrip ipv6 mode

Use **vrrip ipv6 mode** to specify the operating mode for IPv6 VRRP.

Use **undo vrrip ipv6 mode** to restore the default.

Syntax

```
vrrip ipv6 mode load-balance  
undo vrrip ipv6 mode
```

Default

IPv6 VRRP operates in standard mode.

Views

System view

Predefined user roles

network-admin

Parameters

load-balance: Specifies the load balancing mode.

Usage guidelines

When IPv6 VRRP operates in load balancing mode, the virtual IPv6 address of an IPv6 VRRP group cannot be the same as the IPv6 address of the interface where the VRRP group is configured. If the IPv6 addresses are the same, the load balancing mode cannot function.

After you create IPv6 VRRP groups on the router, you can specify their operating mode through this command. All IPv6 VRRP groups on the router operate in the specified mode.

Examples

```
# Specify the load balancing mode for IPv6 VRRP.
<Sysname> system-view
[Sysname] vrrp ipv6 mode load-balance
```

Related commands

display vrrp ipv6

vrrp ipv6 vrid

Use **vrrp ipv6 vrid** to create an IPv6 VRRP group and assign a virtual IPv6 address to the VRRP group or to assign a virtual IPv6 address to an existing IPv6 VRRP group.

Use **undo vrrp ipv6 vrid** to remove all configurations of an existing IPv6 VRRP group or to remove a virtual IPv6 address from an existing IPv6 VRRP group.

Syntax

vrrp ipv6 vrid *virtual-router-id* **virtual-ip** *virtual-address* [**link-local**]

undo vrrp ipv6 vrid *virtual-router-id* [**virtual-ip** [*virtual-address* [**link-local**]]]

Default

No IPv6 VRRP group is created.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

virtual-ip *virtual-address*: Specifies a virtual IPv6 address. If you do not specify this option, the **undo vrrp ipv6 vrid** command removes all virtual IPv6 addresses from the existing IPv6 VRRP group.

link-local: Specifies a link-local address as the virtual IPv6 address.

Usage guidelines

You can assign up to 16 virtual IPv6 addresses to an IPv6 VRRP group.

The first virtual IPv6 address that you assign for an IPv6 VRRP group must be a link-local address, and it must be removed last.

An IPv6 VRRP group can have only one link-local address as its virtual IPv6 address.

If you create an IPv6 VRRP group but do not assign any virtual IPv6 address for it, the VRRP group stays in inactive state and does not function.

The virtual IPv6 address of an IPv6 VRRP group and the downlink interface IPv6 address of the VRRP group must be in the same subnet. Otherwise, the hosts in the subnet might fail to access external networks.

Examples

```
# Create IPv6 VRRP group 1 and assign virtual IPv6 address fe80::10 to the VRRP group. Then assign
virtual IPv6 address 1::10 to the VRRP group.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip 1::10
```

Related commands

display vrrp ipv6

vrrp ipv6 vrid preempt-mode

Use **vrrp ipv6 vrid preempt-mode** to enable the preemptive mode for the router in an IPv6 VRRP group and configure the preemption delay time.

Use **undo vrrp ipv6 vrid preempt-mode** to disable the preemptive mode for the router in an IPv6 VRRP group.

Use **undo vrrp ipv6 vrid preempt-mode delay** to restore the default preemption delay.

Syntax

vrrp ipv6 vrid *virtual-router-id* **preempt-mode** [**delay** *delay-value*]

undo vrrp ipv6 vrid *virtual-router-id* **preempt-mode** [**delay**]

Default

The router operates in preemptive mode and the preemption delay is 0 centiseconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

delay *delay-value*: Specifies a preemption delay time in the range of 0 to 180000 in centiseconds. The default setting is 0 centiseconds.

Usage guidelines

In non-preemptive mode, when a router in the IPv6 VRRP group becomes the master, it acts as the master as long as it operates correctly, even if a backup is assigned a higher priority later. The non-preemptive mode helps avoid frequent switchover between the master and backups.

In preemptive mode, a backup takes over as the master and sends VRRP advertisements when it detects that it has a higher priority than the master. The previous master then becomes a backup. This mechanism makes sure the master is always the router with the highest priority.

To avoid frequent state changes among members in a VRRP group and to provide the backups enough time to collect information (such as routing information), a backup does not immediately become the master after it receives an advertisement with lower priority than the local priority. Instead, it waits for a period of time before taking over as the master.

Examples

Enable the preemptive mode for VRRP group 1, and set the preemption delay time to 500 centiseconds.

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

```
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 10 preempt-mode delay 500
```

Related commands

display vrrp ipv6

vrrp ipv6 vrid priority

Use **vrrp ipv6 vrid priority** to configure the priority of the router in an IPv6 VRRP group.

Use **undo vrrp ipv6 vrid priority** to restore the default.

Syntax

vrrp ipv6 vrid *virtual-router-id* **priority** *priority-value*

undo vrrp ipv6 vrid *virtual-router-id* **priority**

Default

The priority of a router in an IPv6 VRRP group is 100.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

priority-value: Specifies a priority value in the range of 1 to 254. A higher number indicates a higher priority.

Usage guidelines

VRRP determines the role (master or backup) of each router in a VRRP group by priority. A router with a higher priority is more likely to become the master.

VRRP priority is in the range of 0 to 255, and a greater number represents a higher priority. Priorities 1 to 254 are configurable. Priority 0 is reserved for special uses, and priority 255 is for the IP address owner. The router acting as the IP address owner in a VRRP group always has a running priority of 255 and acts as the master as long as it operates correctly.

Examples

Configure the priority of the switch in VRRP group 1 on VLAN-interface 2 as 150.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 priority 150
```

Related commands

display vrrp ipv6

vrrp ipv6 vrid shutdown

Use **vrrp ipv6 vrid shutdown** to disable an IPv6 VRRP group.

Use **undo vrrp ipv6 vrid shutdown** to restore the default.

Syntax

vrrp ipv6 vrid *virtual-router-id* **shutdown**
undo vrrp ipv6 vrid *virtual-router-id* **shutdown**

Default

An IPv6 VRRP group is enabled.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

Usage guidelines

You can use this command to temporarily disable an IPv6 VRRP group. After this command is configured, the VRRP group stays in initialized state, and its configurations remain unchanged. You can change its configuration, and your changes take effect when you enable the VRRP group again.

Examples

```
# Disable IPv6 VRRP group 1.  
<Sysname> system-view  
[Sysname] interface vlan-interface 2  
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 shutdown
```

vrrp ipv6 vrid timer advertise

Use **vrrp ipv6 vrid timer advertise** to configure the interval at which the master in an IPv6 VRRP group sends VRRP advertisements.

Use **undo vrrp ipv6 vrid timer advertise** to restore the default.

Syntax

vrrp ipv6 vrid *virtual-router-id* **timer advertise** *adver-interval*
undo vrrp ipv6 vrid *virtual-router-id* **timer advertise**

Default

The master in an IPv6 VRRP group sends VRRP advertisements at an interval of 100 centiseconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group by its virtual router ID in the range of 1 to 255.

advert-interval: Specifies an interval for the master in the specified IPv6 VRRP group to send VRRP advertisements, in the range of 100 to 4095 centiseconds.

Usage guidelines

The master in an IPv6 VRRP group periodically sends VRRP advertisements to declare its presence. You can use this command to configure the interval at which the master sends VRRP advertisements.

HP recommends that you set the VRRP advertisement interval to be greater than 100 centiseconds to maintain system stability.

The routers in an IPv6 VRRP group can have different intervals for sending VRRP advertisements. The master in the VRRP group sends VRRP advertisements at the specified interval and carries the interval attribute in the advertisements. After a backup receives the advertisement, it records the interval in the advertisement. If the backup does not receive a new VRRP advertisement from the master when the timer ($3 \times \text{VRRP advertisement sending interval} + \text{Skew_Time}$) expires, it regards the master as failed and takes over as the master.

Large network traffic might disable a backup from receiving VRRP advertisements from the master within the specified time and trigger an unexpected master switchover. To solve this problem, you can use this command to configure a larger interval.

Examples

```
# Configure the master in IPv6 VRRP group 1 to send VRRP advertisements at an interval of 500 centiseconds.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 timer advertise 500
```

Related commands

display vrrp ipv6

vrrp ipv6 vrid track

Use **vrrp ipv6 vrid track** to associate an IPv6 VRRP group with a track entry and control master switchover or AVF switchover in the VRRP group in response to changes (such as uplink state changes) detected by the track entry.

Use **undo vrrp ipv6 vrid track** to remove the association between an IPv6 VRRP group and a track entry. If no track entry is specified, the association between the VRRP group and any track entry is removed.

Syntax

```
vrrp ipv6 vrid virtual-router-id track track-entry-number { forwarder-switchover member-ip ipv6-address | priority reduced [ priority-reduced ] | switchover | weight reduced [ weight-reduced ] }
```

```
undo vrrp ipv6 vrid virtual-router-id track [ track-entry-number [ forwarder-switchover | priority reduced | switchover | weight reduced ] ]
```

Default

An IPv6 VRRP group is not associated with any track entry.

Views

Interface view

Predefined user roles

network-admin

Parameters

virtual-router-id: Specifies an IPv6 VRRP group number in the range of 1 to 255.

track-entry-number: Specifies a track entry. The *track-entry-number* argument is in the range of 1 to 1024.

forwarder-switchover member-ip *ipv6-address*: Enables the LVF on the router to take over the role of the AVF at the specified IPv6 address immediately after the specified track entry changes to the negative state. You can use the **display vrrp verbose** command to view the IPv6 addresses of VFs.

priority reduced *priority-reduced*: Reduces the priority of the router in the VRRP group by a specific value when the state of the specified track entry changes to negative. The *priority-reduced* argument is in the range of 1 to 255, and the default is 10.

switchover: Enables the router in backup state to take over as the master immediately after the specified track entry changes to the negative state.

weight reduced *priority-reduced*: Reduces the weight of all VFs on the router in the VRRP group by a specific value when the state of the specified track entry changes to negative. The *weight-reduced* argument is in the range of 1 to 255, and the default is 30.

Usage guidelines

When the associated track entry changes to the negative state, one of the following conditions occurs, depending on your configuration:

- The priority of the router in the VRRP group decreases by a specific value.
- The weight of VFs decreases by a specific value.
- The router immediately takes over as the master if it is a backup.
- The LVF on the router takes over the role of the AVF at the specified IPv6 address immediately.

Before executing this command, create an IPv6 VRRP group on the interface and assign a virtual IPv6 address to it.

The **forwarder-switchover member-ip** *ipv6-address* or **weight reduced** *weight-reduced* option takes effect only when the IPv6 VRRP group is operating in load balancing mode.

If the **priority reduced** keyword is specified but the *priority-reduced* argument is not specified, the priority of the router in the IPv6 VRRP group decreases by 10 when the track entry changes to **negative**.

If the **weight reduced** keyword is specified but the *weight-reduced* argument is not specified, the weight of the VFs on the router in the IPv6 VRRP group decreases by 30 when the track entry changes to **negative**.

The weight of a VF is 255, and its lower limit of failure is 10.

When the weight of a VF owner is higher than or equal to the lower limit of failure, its priority is always 255 and does not change with the weight. To guarantee that an LVF can take over the VF owner as the AVF when the upstream link of the VF owner fails, the reduced weight for the VF owner must be higher than 245 so the weight of the VF owner can drop below the lower limit of failure.

When the track entry changes from Negative to Positive or NotReady, the router automatically restores its priority or VF weight. The failed master router becomes the master again, or the failed AVF becomes active again.

! **IMPORTANT:**

- The **vrrip ipv6 vrid track priority reduced** or **vrrip ipv6 vrid track switchover** command cannot take effect on an IP address owner. If you have configured the command on an IP address owner, the configuration takes effect after the router changes to be a non-IP address owner.
- You can create a track entry with the **track** command before or after you associate it with an IPv6 VRRP group. For more information about configuring track entries, see *High Availability Configuration Guide*.

Examples

Associate IPv6 VRRP group 1 on VLAN-interface 2 with track entry 1 and decrease the priority of the router in the VRRP group by 50 when the state of track entry 1 changes to negative.

```
<Sysname> system-view
[Sysname] interface Vlan-interface2
[Sysname-Vlan-interface2] vrrip vrid 1 track 1 priority reduced 50
```

Associate IPv6 VRRP group 1 on VLAN-interface 2 with track entry 1 and enable the VF in listening state whose AVF is on the member device with the IPv6 address of 11::22 to take over immediately after the specified track entry changes to the negative state.

```
[Sysname-Vlan-interface2] vrrip ipv6 vrid 1 track 1 forwarder-switchover member-ip 11::22
```

Associate IPv6 VRRP group 1 on VLAN-interface 2 with track entry 1 and decrease the weight of all VFs on the router in the IPv6 VRRP group by 50 when the state of track entry 1 changes to negative.

```
[Sysname-Vlan-interface2] vrrip ipv6 vrid 1 track 1 weight reduced 50
```

Related commands

display vrrip ipv6

BFD commands

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

bfd authentication-mode

Use **bfd authentication-mode** to configure the BFD authentication mode for single-hop BFD control packets.

Use **undo bfd authentication-mode** to restore the default.

Syntax

```
bfd authentication-mode { m-md5 | m-sha1 | md5 | sha1 | simple } key-id { cipher cipher-string | plain plain-string }
```

```
undo bfd authentication-mode
```

Default

Single-hop BFD control packets are not authenticated.

Views

Interface view, BFD template view

Predefined user roles

network-admin

Parameters

m-md5: Specifies the Meticulous MD5 algorithm.

m-sha1: Specifies the Meticulous SHA1 algorithm.

md5: Specifies the MD5 algorithm.

sha1: Specifies the SHA1 algorithm.

simple: Specifies the simple authentication mode.

key-id: Sets the authentication key ID in the range of 1 to 255.

cipher: Sets a ciphertext password.

cipher-string: Ciphertext password, which is a case-sensitive string of 33 to 53 characters.

plain: Sets a ciphertext password.

plain-string: Plaintext password, which is a case-sensitive string of 1 to 16 characters.

Usage guidelines

Use this command to enhance BFD session security.

For security purposes, all authentication passwords, including passwords configured in plain text, are saved in cipher text.

Examples

Configure VLAN-interface 11 to perform simple authentication for single-hop BFD control packets, setting the authentication key ID to **1** and password to **123456**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] bfd authentication-mode simple 1 plain 123456
```

bfd demand enable

Use **bfd demand enable** to enable the Demand BFD session mode.

Use **undo bfd demand enable** to restore the default.

Syntax

bfd demand enable

undo bfd demand enable

Default

The BFD session is in Asynchronous mode.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

In Demand mode, the device periodically sends BFD control packets. If the peer end is operating in Asynchronous mode (default), the peer end stops sending BFD control packets. If the peer end is operating in Demand mode, both ends stop sending BFD control packets. When the connectivity to another system needs to be verified explicitly, a system sends several BFD control packets that have the Poll (P) bit set at the negotiated transmit interval. If no response is received within the detection interval, the session is considered down. If the connectivity is found to be up, no more BFD control packets are sent until the next command is issued.

In Asynchronous mode, the device periodically sends BFD control packets. The device considers that the session is down if it does not receive any BFD control packets within a specific interval.

Examples

Enable the Demand BFD session mode on VLAN-interface 11.

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] bfd demand enable
```

bfd detect-interface

Use **bfd detect-interface source-ip** to create a BFD session for detecting the local interface state.

Use **undo bfd detect-interface** to remove the BFD session.

Syntax

bfd detect-interface source-ip *ip-address*

undo bfd detect-interface

Default

No BFD session is created for detecting the local interface state.

Views

Interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the source IP address for BFD control packets.

Usage guidelines

The member ports in Layer 3 aggregation groups do not have IP addresses, and they do not support fast detection mechanisms. You can use this command to detect link faults and locate faulty member ports of Layer 3 aggregate interfaces. You can also configure this command for common Layer 3 Ethernet interfaces to implement fast collaboration between interface state and BFD session state, and help routing protocols complete convergence.

Before you configure this command, you must enable the BFD control packet mode on both ends of the BFD session. The destination IP address for BFD control packets is 224.0.0.184, and it cannot be configured.

HP recommends that you configure the IP address of the interface as the source IP address. If the interface has no IP address configured, configure a unicast address other than 0.0.0.0.

Examples

```
# Create a BFD session to detect the state of interface FortyGigE 1/1/1, and specify the source IP address as 20.1.1.1.
```

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

```
[Sysname] interface fortygige 1/1/1
```

```
[Sysname-FortyGigE1/1/1] bfd detect-interface source-ip 20.1.1.1
```

bfd detect-multiplier

Use **bfd detect-multiplier** to configure the single-hop detection time multiplier.

Use **undo bfd detect-multiplier** to restore the default.

Syntax

```
bfd detect-multiplier value
```

```
undo bfd detect-multiplier
```

Default

The single-hop detection time multiplier is 5.

Views

Interface view

Predefined user roles

network-admin

Parameters

value: Specifies a single-hop detection time multiplier in the range of 3 to 50.

Usage guidelines

The detection time multiplier determines the maximum number of concurrent BFD packets (including control packets and echo packets) that can be discarded.

Table 43 Detection interval calculation method

| Mode | Detection interval |
|--|--|
| Echo packet mode | Detection time multiplier of the sender × actual packet sending interval of the sender |
| Control packet mode BFD session in asynchronous mode | Detection time multiplier of the receiver × actual packet sending interval of the receiver |
| Control packet mode BFD session in demand mode | Detection time multiplier of the sender × actual packet sending interval of the sender |

Examples

```
# Configure the single-hop detection time multiplier as 6 on VLAN-interface 11.
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] bfd detect-multiplier 6
```

bfd echo enable

Use **bfd echo enable** to enable the echo packet mode.

Use **undo bfd echo enable** to restore the default.

Syntax

bfd echo enable

undo bfd echo enable

Default

The echo packet mode is disabled.

Views

Interface view

Predefined user roles

network-admin

Usage guidelines

If you enable the echo packet mode for a BFD session in which control packets are sent and the session comes up, BFD does the following:

- Periodically sends echo packets to detect link connectivity.
- Decreases the control packet receiving rate at the same time.

Examples

```
# Enable the echo packet mode on VLAN-interface 11.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] bfd echo enable
```

bfd echo-source-ip

Use **bfd echo-source-ip** to configure the source IP address of BFD echo packets.

Use **undo bfd echo-source-ip** to remove the configured source IP address of BFD echo packets.

Syntax

```
bfd echo-source-ip ip-address
```

```
undo bfd echo-source-ip
```

Default

No source IP address is configured for BFD echo packets.

Views

System view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the source IP address of BFD echo packets.

Usage guidelines

The source IP address cannot be on the same network segment as any local interface's IP address. Otherwise, a large number of ICMP redirect packets might be sent from the peer, resulting in link congestion.

Examples

```
# Configure the source IP address of BFD echo packets as 8.8.8.8.
```

```
<Sysname> system-view
[Sysname] bfd echo-source-ip 8.8.8.8
```

bfd echo-source-ipv6

Use **bfd echo-source-ipv6** to configure the source IPv6 address of BFD echo packets.

Use **undo bfd echo-source-ipv6** to remove the configured source IPv6 address of BFD echo packets.

Syntax

```
bfd echo-source-ipv6 ipv6-address
```

```
undo bfd echo-source-ipv6
```

Default

No source IPv6 address is configured for BFD echo packets.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the source IPv6 address for BFD echo packets.

Usage guidelines

The source IPv6 address of echo packets can only be a global unicast address.

The source IPv6 address cannot be on the same network segment as any local interface's IP address. Otherwise, a large number of ICMP redirect packets might be sent from the peer, resulting in link congestion.

Examples

```
# Configure the source IPv6 address of BFD echo packets as 80::2.
<Sysname> system-view
[Sysname] bfd echo-source-ipv6 80::2
```

bfd min-echo-receive-interval

Use **bfd min-echo-receive-interval** to configure the minimum interval for receiving BFD echo packets.

Use **undo bfd min-echo-receive-interval** to restore the default.

Syntax

```
bfd min-echo-receive-interval value
undo bfd min-echo-receive-interval
```

Default

The minimum interval for receiving BFD echo packets is 400 milliseconds.

Views

Interface view

Predefined user roles

network-admin

Parameters

value: Specifies a minimum interval for receiving BFD echo packets, in milliseconds. The value takes 0 or is in the range of 100 to 1000.

Usage guidelines

This command sets the BFD echo packet receiving interval, which is the actual BFD echo packet sending interval.

Examples

```
# Configure the minimum interval for receiving BFD echo packets on VLAN-interface 11 as 500
milliseconds.
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] bfd min-echo-receive-interval 500
```

bfd min-receive-interval

Use **bfd min-receive-interval** to configure the minimum interval for receiving single-hop BFD control packets.

Use **undo bfd min-receive-interval** to restore the default.

Syntax

bfd min-receive-interval *value*

undo bfd min-receive-interval

Default

The minimum interval for receiving single-hop BFD control packets is 400 milliseconds.

Views

Interface view, BFD template view

Predefined user roles

network-admin

Parameters

value: Specifies the minimum interval for receiving single-hop BFD control packets, in the range of 100 to 1000 milliseconds.

Usage guidelines

Configure this command to prevent the control packet sending rate of the peer end from exceeding the control packet receiving rate of the local end.

The actual control packet sending interval of the peer end takes the greater value between the minimum interval for transmitting BFD control packets on the peer end and the minimum interval for receiving BFD control packets on the local end.

Examples

Configure the minimum interval for receiving single-hop BFD control packets on VLAN-interface 11 as 500 milliseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] bfd min-receive-interval 500
```

bfd min-transmit-interval

Use **bfd min-transmit-interval** to configure the minimum interval for transmitting single-hop BFD control packets.

Use **undo bfd min-transmit-interval** to restore the default.

Syntax

bfd min-transmit-interval *value*

undo bfd min-transmit-interval

Default

The minimum interval for transmitting single-hop BFD control packets is 400 milliseconds.

Views

Interface view, BFD template view

Predefined user roles

network-admin

Parameters

value: Specifies the minimum interval for transmitting single-hop BFD control packets, in the range of 100 to 1000 milliseconds.

Usage guidelines

Use this command to make sure that the BFD packet sending rate does not exceed the device capability. The actual BFD control packet transmitting interval on the local end is the greater value between the minimum interval for transmitting BFD control packets on the local end and the minimum interval for receiving BFD control packets on the peer end.

Examples

```
# Configure the minimum interval for transmitting single-hop BFD control packets on VLAN-interface 11 as 500 milliseconds.
```

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] bfd min-transmit-interval 500
```

bfd multi-hop authentication-mode

Use **bfd multi-hop authentication-mode** to configure the authentication mode for multihop BFD control packets.

Use **undo bfd multi-hop authentication-mode** to restore the default.

Syntax

```
bfd multi-hop authentication-mode { m-md5 | m-sha1 | md5 | sha1 | simple } key-id { cipher cipher-string | plain plain-string }
```

```
undo bfd multi-hop authentication-mode
```

Default

No authentication is performed.

Views

System view

Predefined user roles

network-admin

Parameters

m-md5: Specifies the Meticulous MD5 algorithm.

m-sha1: Specifies the Meticulous SHA1 algorithm.

md5: Specifies the MD5 algorithm.

sha1: Specifies the SHA1 algorithm.

simple: Specifies the simple authentication mode.

key-id: Sets the authentication key ID in the range of 1 to 255.

cipher: Sets a ciphertext password.

cipher-string: Sets the ciphertext password, which is a case-sensitive string of 33 to 53 characters.

plain: Sets a plaintext password.

plain-string: Sets the plaintext password, which is a case-sensitive string of 1 to 16 characters.

Usage guidelines

Use this command to enhance BFD session security.

For security purposes, all authentication passwords, including passwords configured in plain text, are saved in cipher text.

Examples

```
# Configure the simple authentication mode for multihop BFD control packets, setting the authentication key ID to 1 and password to 123456.
```

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

```
[Sysname] bfd multi-hop authentication-mode simple 1 plain 123456
```

bfd multi-hop destination-port

Use **bfd multi-hop destination-port** to configure the destination port number for multihop BFD control packets.

Use **undo bfd multi-hop destination-port** to restore the default.

Syntax

```
bfd multi-hop destination-port port-number
```

```
undo bfd multi-hop destination-port
```

Default

The destination port number for multihop BFD control packets is 4784.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies the destination port number of multihop BFD control packets, 3784 or 4784.

Examples

```
# Configure the destination port number for multihop BFD control packets as 3784.
```

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

```
[Sysname] bfd multi-hop destination-port 3784
```

bfd multi-hop detect-multiplier

Use **bfd multi-hop detect-multiplier** to configure the multihop detection time multiplier.

Use **undo bfd multi-hop detect-multiplier** to restore the default.

Syntax

```
bfd multi-hop detect-multiplier value  
undo bfd multi-hop detect-multiplier
```

Default

The multihop detection time multiplier is 5.

Views

System view

Predefined user roles

network-admin

Parameters

value: Specifies the multihop detection time multiplier in the range of 3 to 50.

Usage guidelines

The detection time multiplier determines the maximum number of concurrent BFD control packets that can be discarded.

Table 44 Detection interval calculation method

| Mode | Detection interval |
|--|--|
| Control packet mode BFD session in asynchronous mode | Detection time multiplier of the receiver × actual packet sending interval of the receiver |
| Control packet mode BFD session in demand mode | Detection time multiplier of the sender × actual packet sending interval of the sender |

Examples

```
# Configure the multihop detection time multiplier as 6.  
<Sysname> system-view  
[Sysname] bfd multi-hop detect-multiplier 6
```

bfd multi-hop min-receive-interval

Use **bfd multi-hop min-receive-interval** to configure the minimum interval for receiving multihop BFD control packets.

Use **undo bfd multi-hop min-receive-interval** to restore the default.

Syntax

```
bfd multi-hop min-receive-interval value  
undo bfd multi-hop min-receive-interval
```

Default

The minimum interval for receiving multihop BFD control packets is 400 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

value: Specifies the minimum interval for receiving multihop BFD control packets, in the range of 100 to 1000 milliseconds.

Usage guidelines

When the packet sending rate of the peer end exceeds the packet receiving capability (minimum control packet receiving interval) of the local end, the peer end dynamically adjusts the BFD control packet sending interval to the minimum control packet receiving interval of the local end.

Examples

```
# Configure the minimum interval for receiving multihop BFD control packets as 500 milliseconds.
<Sysname> system-view
[Sysname] bfd multi-hop min-receive-interval 500
```

bfd multi-hop min-transmit-interval

Use **bfd multi-hop min-transmit-interval** to configure the minimum interval for transmitting multihop BFD control packets.

Use **undo bfd multi-hop min-transmit-interval** to restore the default.

Syntax

```
bfd multi-hop min-transmit-interval value
undo bfd multi-hop min-transmit-interval
```

Default

The minimum interval for transmitting multihop BFD control packets is 400 milliseconds.

Views

System view

Predefined user roles

network-admin

Parameters

value: Specifies the minimum interval for transmitting multihop BFD control packets, in the range of 100 to 1000 milliseconds.

Usage guidelines

Use this command to make sure that the BFD packet sending rate does not exceed the device capability. The actual BFD control packet transmitting interval on the local end is the greater value between the minimum interval for transmitting BFD control packets on the local end and the minimum interval for receiving BFD control packets on the peer end.

Examples

```
# Configure the minimum interval for transmitting multihop BFD control packets as 500 milliseconds.
<Sysname> system-view
[Sysname] bfd multi-hop min-transmit-interval 500
```

bfd session init-mode

Use **bfd session init-mode** to configure the mode for establishing a BFD session.

Use **undo bfd session init-mode** to restore the default.

Syntax

```
bfd session init-mode { active | passive }
```

```
undo bfd session init-mode
```

Default

BFD uses the **active** mode.

Views

System view

Predefined user roles

network-admin

Parameters

active: Uses the active mode. In active mode, BFD actively transmits BFD control packets to the remote device, regardless of whether it receives a BFD control packet from the remote device.

passive: Uses the passive mode. In passive mode, BFD does not actively transmit a BFD control packet to the remote end; it transmits a BFD control packet only after receiving a BFD control packet from the remote end.

Usage guidelines

At least one end must operate in active mode for a BFD session to be established.

Examples

```
# Configure the session establishment mode as passive.
```

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

```
[Sysname] bfd session init-mode passive
```

bfd template

Use **bfd template** to create a BFD template and enter BFD template view.

Use **undo bfd template** to delete the BFD template.

Syntax

```
bfd template template-name
```

```
undo bfd template template-name
```

Default

No BFD template is created.

Views

System view

Predefined user roles

network-admin

Parameters

template-name: Specifies the template name, a case-sensitive string of 1 to 63 characters.

Examples

```
# Create BFD template bfd1 and enter BFD template view.
<Sysname> system-view
[Sysname] bfd template bfd1
[Sysname-bfd-template-bfd1]
```

display bfd session

Use **display bfd session** to display BFD session information.

Syntax

```
display bfd session [ discriminator value | verbose ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

discriminator value: Specifies a local ID in the range of 1 to 4294967295. If this option is not specified, the command displays brief information about all BFD sessions.

verbose: Displays detailed BFD session information. If this keyword is not specified, the command displays brief BFD session information.

Examples

```
# Display all IPv4 BFD session information.
```

```
<Sysname> display bfd session
```

```
Total Session Num: 1      Up Session Num: 1      Init Mode: Active
```

```
IPv4 Session Working Under Ctrl Mode:
```

| LD/RD | SourceAddr | DestAddr | State | Holdtime | Interface |
|---------|------------|----------|-------|----------|-----------|
| 513/513 | 1.1.1.1 | 1.1.1.2 | Up | 2297ms | FGE1/1/1 |

```
# Display all IPv6 BFD session information.
```

```
<Sysname> display bfd session
```

```
Total Session Num: 1      Up Session Num: 1      Init Mode: Active
```

```
IPv6 Session Working Under Ctrl Mode:
```

```
Local Discr: 513          Remote Discr: 513
Source IP: FE80::20C:29FF:FED4:7171
Destination IP: FE80::20C:29FF:FE72:AC4D
```

```

Session State: Up                               Interface: FGE1/1/2
# Display detailed IPv4 BFD session information.
<Sysname> display bfd session verbose

Total Session Num: 1      Up Session Num: 1      Init Mode: Active

IPv4 Session Working Under Ctrl Mode:

    Local Discr: 513                               Remote Discr: 513
    Source IP: 1.1.1.1                             Destination IP: 1.1.1.2
Session State: Up                               Interface: FortyGigE 1/1/1
Min Tx Inter: 500ms                             Act Tx Inter: 500ms
Min Rx Inter: 500ms                             Detect Inter: 2500ms
    Rx Count: 42                                   Tx Count: 43
Connect Type: Direct                             Running Up for: 00:00:20
    Hold Time: 2078ms                             Auth mode: None
Detect Mode: Async                               Slot: 1
    Protocol: OSPF
    Diag Info: No Diagnostic
Template name: abc

```

Display detailed IPv6 BFD session information.

```

<Sysname> display bfd session verbose

Total Session Num: 1      Up Session Num: 1      Init Mode: Active

IPv6 Session Working Under Ctrl Mode:

    Local Discr: 513                               Remote Discr: 513
    Source IP: FE80::20C:29FF:FED4:7171
Destination IP: FE80::20C:29FF:FE72:AC4D
Session State: Up                               Interface: FortyGigE 1/1/2
Min Tx Inter: 500ms                             Act Tx Inter: 500ms
Min Rx Inter: 500ms                             Detect Inter: 2500ms
    Rx Count: 38                                   Tx Count: 38
Connect Type: Direct                             Running Up for: 00:00:15
    Hold Time: 2211ms                             Auth mode: None
Detect Mode: Async                               Slot: 1
    Protocol: OSPFv3
    Diag Info: No Diagnostic
Template name: abc

```

Table 45 Command output

| Field | Description |
|-------------------|--|
| Total Session Num | Total number of BFD sessions. |
| Up Session Num | Total number of active BFD sessions. |
| Init Mode | BFD operating mode, active or passive. |

| Field | Description |
|---------------------------------|---|
| Session Working Under Ctrl Mode | IPv4/IPv6 BFD session mode: <ul style="list-style-type: none"> • Ctrl—Control packet mode. • Echo—Echo packet mode. |
| Local Discr/LD | Local ID of the session. |
| Remote Discr/RD | Remote ID of the session. |
| Source IP/SourceAddr | Source IP address of the session. |
| Destination IP/DestAddr | Destination IP address of the session. |
| Session State/State | Session state: up or down. |
| Interface | Name of the interface of the session. |
| Min Tx Inter | Minimum transmit interval. |
| Min Rx Inter | Minimum receive interval. |
| Act Tx Inter | Actual transmit interval. |
| Detect Inter | Actual session detection timer. |
| Rx Count | Number of packets received. |
| Tx Count | Number of packets sent. |
| Hold Time/Holdtime | Length of time before session detection timer expires. |
| Auth mode | Session authentication mode (only simple is supported). |
| Connect Type | Connection type of the interface, direct or indirect. |
| Running up for | Time interval for which the session has been up. |
| Detect Mode | Detection mode: <ul style="list-style-type: none"> • Async—Asynchronous mode. • Demand—Demand mode. |
| Slot | IRF member ID. |
| Diag Info | Diagnostic information about the session. |
| Template name | BFD template name. |

reset bfd session statistics

Use **reset bfd session statistics** to clear the BFD session statistics.

Syntax

```
reset bfd session statistics
```

Views

User view

Predefined user roles

network-admin

Examples

```
# Clear the BFD session statistics.
```



```
<Sysname> reset bfd session statistics
```

Track commands

display track

Use **display track** to display track entry information.

Syntax

```
display track { track-entry-number | all }
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

all: Specifies all track entries.

Examples

Display information about all track entries.

```
<Sysname> display track all
Track ID: 1
  State: Positive
  Duration: 0 days 0 hours 0 minutes 7 seconds
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    NQA entry: admin test
    Reaction: 10
Track ID: 2
  State: NotReady
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    BFD session mode: Echo
    Outgoing interface: Vlan-interface2
    VPN instance name: -
    Remote IP: 192.168.40.1
    Local IP: 192.168.40.2
Track ID: 3
  State: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    Interface: Vlan-interface3
```

```

Protocol: IPv4
Track ID: 4
State: Negative
Duration: 0 days 0 hours 0 minutes 32 seconds
Notification delay: Positive 20, Negative 30 (in seconds)
Tracked object:
CFD service instance: 1, MEP ID: 2

```

Table 46 Command output

| Field | Description |
|---|--|
| Track ID | ID of a track entry. |
| State | States of a track entry: <ul style="list-style-type: none"> • Positive—The tracked object operates correctly. • NotReady—The tracked object is invalid. • Negative—The tracked object is abnormal. |
| Duration | Time period during which the track entry stays in the state. |
| Notification delay: Positive 20, Negative 30 (in seconds) | <ul style="list-style-type: none"> • The Track module notifies the application modules that the status of the track entry changes to Positive after a delay time of 20 seconds. • The Track module notifies the application modules that the status of the track entry changes to Negative after a delay time of 30 seconds. |
| Tracked object | Tracked object associated with the track entry. |
| NQA entry | NQA operation associated with the track entry. |
| Reaction | Reaction entry associated with the track entry. |
| BFD session mode | BFD session mode. Only echo mode is supported. |
| Outgoing interface | Output interface of BFD echo packets. |
| VPN instance name | Name of VPN instance to which BFD session packets belong. If the packets belong to a public network, a hyphen (-) is displayed. |
| Remote IP | Remote IP address of the BFD echo packets. |
| Local IP | Local IP address of the BFD echo packets. |
| Interface | Interface to be monitored. |
| Protocol | Link states or Layer 3 protocol states of the monitored interface: <ul style="list-style-type: none"> • None—Link status of the monitored interface. • IPv4—IPv4 protocol status of the monitored Layer 3 interface. • IPv6—IPv6 protocol status of the monitored Layer 3 interface. |

Related commands

- **track bfd**
- **track cfd**
- **track interface**
- **track interface protocol**
- **track nqa**

track bfd

Use **track bfd** to create a track entry and associate it with a BFD session.

Use **undo track** to remove the track entry.

Syntax

```
track track-entry-number bfd echo interface interface-type interface-number remote ip remote-ip local ip local-ip [ delay { negative negative-time | positive positive-time } * ]
```

```
undo track track-entry-number
```

Default

No track entry exists.

Views

System view

Predefined user roles

network-admin

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

interface *interface-type interface-number*: Specifies the output interface by its type and number of the BFD echo packets.

remote ip *remote-ip*: Specifies the destination IP address of the BFD echo packets.

local ip *local-ip*: Specifies the source IP address of the BFD echo packets.

delay: Specifies the delay before the Track module notifies the application modules of the track entry state change. If you do not specify this keyword, the Track module notifies the application modules immediately when the track entry state changes.

negative *negative-time*: Specifies the delay before the Track module notifies the application modules that the status of the track entry has changed to Negative. The *negative-time* argument represents the delay time in the range of 1 to 300 seconds.

positive *positive-time*: Specifies the delay before the Track module notifies the application modules that the status of the track entry has changed to Positive. The *positive-time* argument represents the delay time in the range of 1 to 300 seconds.

Usage guidelines

After a track entry is created, you can only use the **track bfd delay** command to modify its notification delay settings. To modify other settings, you must delete the entry and create a new one.

When you configure collaboration between Track and BFD, do not configure the virtual IP address of a VRRP group as the local or remote address of a BFD session.

Examples

```
# Create track entry 1, which uses BFD to monitor the link between local IP address 1.1.1.2 and remote IP address 1.1.1.1 by sending BFD echo packets out from the VLAN-interface 2.
```

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

```
[Sysname] track 1 bfd echo interface vlan-interface 2 remote ip 1.1.1.1 local ip 1.1.1.2
```

Related commands

display track

track cfd

Use **track cfd** to create a track entry and associate it with CFD.

Use **undo track** to remove the track entry.

Syntax

```
track track-entry-number cfd cc service-instance instance-id mep mep-id [ delay { negative negative-time | positive positive-time } * ]
```

```
undo track track-entry-number
```

Default

No track entry exists.

Views

System view

Predefined user roles

network-admin

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

service-instance *instance-id*: Specifies a service instance by its ID in the range of 1 to 32767.

mep *mep-id*: Specifies a MEP by its ID in the range of 1 to 8191.

delay: Specifies the delay before the Track module notifies the application modules of the track entry state change. If you do not specify this keyword, the Track module notifies the application modules immediately when the track entry state changes.

negative *negative-time*: Specifies the delay before the Track module notifies the application modules that the status of the track entry has changed to Negative. The *negative-time* argument represents the delay time in the range of 1 to 300 seconds.

positive *positive-time*: Specifies the delay before the Track module notifies the application modules that the status of the track entry has changed to Positive. The *positive-time* argument represents the delay time in the range of 1 to 300 seconds.

Usage guidelines

After a track entry is created, you can only use the **track cfd delay** command to modify its notification delay settings. To modify other settings, you must delete the entry and create a new one.

Examples

```
# Create track entry 1, and specify the CFD service instance ID as 2 and MEP ID as 3.  
<Sysname> system-view  
[Sysname] track 1 cfd cc service-instance 2 mep 3
```

Related commands

- **display track**
- **cfd mep**

- **cfg service-instance**

track interface

Use **track interface** to create a track entry and associate it with the link state of the specified interface.

Use **undo track** to remove the track entry.

Syntax

```
track track-entry-number interface interface-type interface-number [ delay { negative negative-time | positive positive-time } * ]
```

```
undo track track-entry-number
```

Default

No track entry exists.

Views

System view

Predefined user roles

network-admin

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

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

delay: Specifies the delay before the Track module notifies the application modules of the track entry state change. If you do not specify this keyword, the Track module notifies the application modules immediately when the track entry state changes.

negative *negative-time*: Specifies the delay before the Track module notifies the application modules that the state of the track entry has changed to Negative. The *negative-time* argument represents the delay time in the range of 1 to 300 seconds.

positive *positive-time*: Specifies the delay before the Track module notifies the application modules that the state of the track entry has changed to Positive. The *positive-time* argument represents the delay time in the range of 1 to 300 seconds.

Usage guidelines

When you create a track entry that is associated with the link state of a specific interface, the state of the track entry is Positive if the link state of the interface is up. The state of the track entry is Negative if the link state of the interface is down.

To display the link state of an interface, use the **display ip interface brief** command.

After you create a track entry, you can only use the **track interface delay** command to modify its notification delay settings. To modify other settings, you must delete the entry and create a new one.

Examples

```
# Create track entry 1, and associate it with the link state of VLAN-interface 10.
```

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

```
[Sysname] track 1 interface vlan-interface 10
```

Related commands

- **display track**
- **display ip interface brief** (*Layer 3—IP Services Command Reference*)

track interface protocol

Use **track interface protocol** to create a track entry and associate it with the protocol state of the specified interface.

Use **undo track** to remove the track entry.

Syntax

```
track track-entry-number interface interface-type interface-number protocol { ipv4 | ipv6 } [ delay  
{ negative negative-time | positive positive-time } * ]
```

```
undo track track-entry-number
```

Default

No track entry exists.

Views

System view

Predefined user roles

network-admin

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

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

ipv4: Monitors the IPv4 protocol state. When the IPv4 protocol state of an interface is up, the state of the track object is Positive. When the IPv4 protocol state of an interface is down, the state of the track object is Negative. To display the IPv4 protocol state of an interface, use the **display ip interface brief** command.

ipv6: Monitors the IPv6 protocol state. When the IPv6 protocol state of an interface is up, the state of the track object is Positive. When the IPv6 protocol state of an interface is down, the state of the track object is Negative. To display the IPv6 protocol state of an interface, use the **display ipv6 interface brief** command.

delay: Specifies the delay before the Track module notifies the application modules of the track entry state change. If you do not specify this keyword, the Track module notifies the application modules immediately when the track entry state changes.

negative *negative-time*: Specifies the delay before the Track module notifies the application modules that the state of the track entry has changed to Negative. The *negative-time* argument represents the delay time in the range of 1 to 300 seconds.

positive *positive-time*: Specifies the delay before the Track module notifies the application modules that the state of the track entry has changed to Positive. The *positive-time* argument represents the delay time in the range of 1 to 300 seconds.

Usage guidelines

After a track entry is created, you can only use the **track interface protocol delay** command to modify its notification delay settings. To modify other settings, you must delete the entry and create a new one.

Examples

```
# Create track entry 1, and associate it with the IPv4 protocol state of VLAN-interface 2.
<Sysname> system-view
[Sysname] track 1 interface vlan-interface 2 protocol ipv4
```

Related commands

- **display track**
- **display ip interface brief** (*Layer 3—IP Services Command Reference*)
- **display ipv6 interface brief** (*Layer 3—IP Services Command Reference*)

track nqa

Use **track nqa** to create a track entry and associate it with the specified reaction entry of the NQA operation.

Use **undo track** to remove the track entry.

Syntax

```
track track-entry-number nqa entry admin-name operation-tag reaction item-number [ delay { negative negative-time | positive positive-time } * ]
```

```
undo track track-entry-number
```

Default

No track entry exists.

Views

System view

Predefined user roles

network-admin

Parameters

track-entry-number: Specifies the track entry ID in the range of 1 to 1024.

entry *admin-name operation-tag*: Specifies the NQA operation to be associated with the track entry. The *admin-name* argument is the name of the NQA operation administrator who creates the NQA operation, and is a case-insensitive string of 1 to 32 characters. The *operation-tag* argument is the NQA operation tag, a case-insensitive string of 1 to 32 characters.

reaction *item-number*: Specifies the reaction entry to be associated with the track entry. The *item-number* argument is the reaction entry ID in the range of 1 to 10.

delay: Specifies the delay before the Track module notifies the application modules of the track entry state change. If you do not specify this keyword, the Track module notifies the application modules immediately when the track entry state changes.

negative *negative-time*: Specifies the delay before the Track module notifies the application modules that the state of the track entry has changed to Negative. The *negative-time* argument represents the delay time in the range of 1 to 300 seconds.

positive *positive-time*: Specifies the delay before the Track module notifies the application modules that the state of the track entry has changed to Positive. The *positive-time* argument represents the delay time in the range of 1 to 300 seconds.

Usage guidelines

After a track entry is created, you can only use the **track nqa delay** command to modify its notification delay settings. To modify other settings, you must delete the entry and create a new one.

Examples

Create track entry 1, and associate it with reaction entry 3 of the NQA operation **admin-test**.

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

```
[Sysname] track 1 nqa entry admin test reaction 3
```

Related commands

display track

Process placement commands

affinity location-set

Use **affinity location-set** to set the affinity of a process to a set of CPUs.

Use **undo affinity location-set** to remove the configuration.

Syntax

```
affinity location-set { slot slot-number [ cpu cpu-number ] }&<1-5> { attract strength | default | none | repulse strength }
```

```
undo affinity location-set { slot slot-number [ cpu cpu-number ] }&<1-5>
```

Default

No location affinity is configured for any process.

Views

Placement process view

Predefined user roles

network-admin

Parameters

{ **slot** *slot-number* [**cpu** *cpu-number*] }&<1-5>: Specifies the affinity.

- **slot** *slot-number*: Specifies an IRF member device by its ID.
- **cpu** *cpu-number*: Specifies a CPU by its number. The number can only be 0.

attract *strength*: Sets a positive affinity in the range of 1 to 100000. The higher the value, the stronger the preference for the process to run in the specified CPU.

default: Sets the affinity to the default, a positive affinity of 200.

none: Sets the affinity to 0, which means the active process has no preference for any location and the system determines its location.

repulse *strength*: Sets a negative affinity in the range of 1 to 100000. The higher the value, the weaker the preference for the process to run in the specified CPU.

Usage guidelines

This command sets the preference for a process to run on a specific CPU. You can specify up to five CPUs in this command.

Examples

```
# Configure a positive affinity of 500 to IRF member device 3 for BGP.  
<Sysname> system-view  
[Sysname] placement program bgp  
[Sysname-program-bgp] affinity location-set slot 3 attract 500
```

affinity location-type

Use **affinity location-type** to set the affinity of a process to a location type.

Use **undo affinity location-type** to restore the default.

Syntax

```
affinity location-type { current | paired | primary } { attract strength | default | none | repulse strength }  
undo affinity location-type { current | paired | primary }
```

Default

No location type affinity is configured for any process.

Views

Placement process view

Predefined user roles

network-admin

Parameters

current: Specifies the affinity to the current location. You can use the **display placement program** command to view the current location of a process.

paired: Specifies the affinity to the location of a standby process.

primary: Specifies the affinity to the master device.

attract *strength*: Sets a positive affinity in the range of 1 to 100000. The higher the value, the stronger the preference of the process to run on the specified location type.

default: Sets the affinity to the default, a positive affinity of 200.

none: Sets the affinity to 0.

repulse *strength*: Sets a negative affinity in the range of 1 to 100000. The higher the value, the weaker the preference for the process to run on the specified location type.

Examples

```
# Specify a positive affinity of 500 to the current location for BGP.  
<Sysname> system-view  
[Sysname] placement program bgp  
[Sysname-program-bgp] affinity location-type current attract 500
```

Related commands

- **affinity location-set**
- **affinity program**

affinity program

Use **affinity program** to set the affinity of one process to another process.

Use **undo affinity program** to remove the configuration.

Syntax

```
affinity program program-name { attract strength | default | none | repulse strength }
```

undo affinity program *program-name*

Default

No process affinity is configured for any process.

Views

Placement process view

Predefined user roles

network-admin

Parameters

program-name: Specifies the name of a process, a case-insensitive string of 1 to 15 characters. You can use the **display placement program all** command to view information about placeable processes.

attract strength: Sets a positive affinity in the range of 1 to 100000. The higher the value, the stronger the preference for the current process to run on the same location as the specified process.

default: Sets the affinity to the default, a positive affinity of 200.

none: Sets the affinity to 0, which means the active process has no preference for any other process and the system determines its location.

repulse strength: Sets a negative affinity in the range of 1 to 100000. The higher the value, the weaker the preference for the current process to run on the same location as the specified process.

Usage guidelines

Use this command to have processes run on the same location or different locations.

Examples

```
# Configure a negative affinity of 200 for OSPF to run on the same location as BGP.
<Sysname> system-view
[Sysname] placement program ospf
[Sysname-program-ospf] affinity program bgp repulse 200
```

Related commands

- **affinity location-set**
- **affinity location-type**

affinity self

Use **affinity self** to set the affinity of one instance of a process to any other instance of the same process.

Use **undo affinity self** to remove the configuration.

Syntax

affinity self { **attract strength** | **default** | **none** | **repulse strength** }

undo affinity self

Default

No self affinity is configured for any process.

Views

Placement process view

Predefined user roles

network-admin

Parameters

attract *strength*: Specifies a positive affinity in the range of 1 to 100000. The higher the value, the stronger the preference for all the instances of the current process to run on the same location.

default: Sets the affinity to the default, a positive affinity of 200.

none: Sets the affinity to 0, which means the instances of the process have no preference to run on the same location and the system determines their locations.

repulse *strength*: Sets a negative affinity in the range of 1 to 100000. The higher the value, the weaker the preference for all the instances of the current process to run on the same location.

Usage guidelines

This command sets the preference for a process to run all its instances on the same location or different locations. If the process has only one instance, the command does not take effect.

The self affinity in the placement process view of a process and any of its instances overwrite each other, and whichever is configured the last takes effect on all the instances of the process.

To view the instances of a process, use the **display placement program all** command.

Examples

```
# Configure a negative self affinity of 200 for BGP.  
<Sysname> system-view  
[Sysname] placement program bgp  
[Sysname-program-bgp] affinity self repulse 200
```

Related commands

- **affinity location-set**
- **affinity location-type**

display ha service-group

Use **display ha service-group** to display the location and status of a service group.

Syntax

```
display ha service-group { program-name [ instance instance-name ] | all }
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

program-name: Specifies a service group by its name, a case-insensitive string of 1 to 15 characters.

all: Specifies all service groups running on the device.

instance *instance-name*: Specifies an instance by its name, a case-insensitive string of 1 to 15 characters. Whether or not a service group has multiple instances depends on the system software.

Examples

Display the location and status of all service groups.

```
<Sysname> display ha service-group all
```

| Service Group | Current Location | State |
|---------------|------------------|-----------------|
| ospf | 1/0 | Realtime Backup |
| bgp | 1/0 | Batch Backup |
| isis | 1/0 | Stopping |
| rip | 1/0 | Realtime Backup |
| ripng | 1/0 | Upgrading |
| staticroute | 1/0 | Batch Backup |

Display the location and status of the specified service group.

```
<Sysname> display ha service-group staticroute
```

| Service Group | Current Location | State |
|---------------|------------------|--------------|
| staticroute | 1/0 (Active) | Batch Backup |

Detailed information about services of the program:

| Service | PID | Type | Location | State |
|-------------|-----|---------|----------|-----------------|
| ifm | 200 | Active | 1/0 | Realtime Backup |
| staticroute | 200 | Active | 1/0 | Batch Backup |
| ifm | 200 | Standby | 2/0 | Realtime Backup |
| staticroute | 200 | Standby | 2/0 | Batch Backup |

The output shows the following:

- The active process of the service group **staticroute** is running on CPU 0 of IRF member device 1, and is in batch backup state.
- The standby process is running on CPU 0 of IRF member device 2.
- The service group has two services **ifm** and **staticroute** with PID **200**. **ifm** is in real-time backup state, and **staticroute** is in batch backup state.

Table 47 Command output

| Field | Description |
|---------------|---|
| Service Group | Service group name. |
| Type | Process type: active or standby. |
| Service | Service name. |
| State | Process status: <ul style="list-style-type: none">• Realtime Backup• Batch Backup• Stopping• Degrading• Upgrading |

display placement location

Use **display placement location** to display the processes running on a specific location.

Syntax

```
display placement location { all | slot slot-number [ cpu cpu-number ] }
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all: Displays all processes running on the device.

slot *slot-number*: Displays the processes running on an IRF member device. The *slot-number* argument specifies the ID of the IRF member device.

cpu *cpu-number*: Specifies a CPU by its number. The number can only be 0.

Examples

```
# Display the processes running on IRF member device 1.
```

```
<Sysname> display placement location slot 1
```

```
Program(s) placed at location: 1/0
```

```
  l3vpn
```

```
  lsm
```

```
  aaa
```

```
  lauth
```

```
  track
```

```
  bfd
```

```
  rm6
```

```
  rm
```

```
  rpm
```

```
  usr6
```

```
  ipaddr
```

```
  ip6addr
```

```
  slsp
```

```
  usr
```

```
  ethbase
```

```
  ip6base
```

```
  ipbase
```

```
  eth
```

display placement policy

Use **display placement policy** to display process placement policy information.

Syntax

```
display placement policy program { program-name | all | default }
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

program-name: Displays the placement policy for a process. The process name is a case-insensitive string of 1 to 15 characters.

all: Displays all process placement policies.

default: Displays the default process placement policy. It is not displayed if no default process placement policy is configured with the **placement program default** command.

Usage guidelines

The information about a placement policy is displayed only when the placement policy is configured for the specified process.

Examples

Display the default process placement policy.

```
<Sysname> display placement policy program default
Program: [default]                               : source
-----
  affinity location-set slot 0 cpu 0 attract      : system [default]
```

Display the placement policy for AAA.

```
<Sysname> display placement policy program aaa
Program: aaa                                     : source
-----
  affinity location-set slot 0 cpu 0 attract      : system [default]
  100
```

Table 48 Command output

| Field | Description |
|---------|--|
| Program | Process name. |
| source | Source of the setting. The text system [default] identifies a default placement setting configured in the view you enter with the placement program default command. The text system aaa identifies a placement setting for the process aaa configured in the view you enter with the placement program program-name command. |

display placement program

Use **display placement program** to display the location of an active process.

Syntax

```
display placement program { program-name | all }
```


Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

program-name: Specifies a process by its name, a case-insensitive string of 1 to 15 characters.

all: Specifies all processes.

Examples

Display the location of AAA.

```
<Sysname> display placement program aaa
Program                               Placed at location
-----
aaa                                   1/0
```

Table 49 Command output

| Field | Description |
|--------------------|---|
| Program | Process name. |
| Placed at location | Location of the process. If NA is displayed, the process is not available because the service is abnormal or the process is starting up or shut down. |

display placement reoptimize

Use **display placement reoptimize** to display the predicted changes that will occur when you run the **placement reoptimize** command.

Syntax

```
display placement reoptimize program { program-name [ instance instance-name ] | all }
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

program-name: Displays changes for a process (that supports process optimization) specified by its name, a case-insensitive string of 1 to 15 characters.

instance *instance-name*: Specifies an instance of the specified process by name, a case-insensitive string of 1 to 15 characters. Whether a process has multiple instances depends on the system software.

all: Displays changes for all processes that support process optimization.

Examples

```
# Display the predicted changes for all processes.
```

```
<Sysname> display placement reoptimize program all
```

```
Predicted changes to the placement
```

| Program | Current location | New location |
|---------|------------------|--------------|
| rm6 | 1/0 | 1/0 |
| rm | 1/0 | 1/0 |
| rpm | 1/0 | 1/0 |
| usr | 1/0 | 1/0 |
| usr6 | 1/0 | 1/0 |
| bgp | 1/0 | 1/0 |
| pim | 1/0 | 1/0 |
| igmp | 1/0 | 1/0 |

The output shows the process name, current location of the active process, and new location of the active process after optimization.

placement program

Use **placement program** to enter placement process view.

Use **undo placement program** to delete the placement policy for a process.

Syntax

```
placement program { program-name [ instance instance-name ] | default }
```

```
undo placement program { program-name [ instance instance-name ] | default }
```

Default

No placement process view is created, and all active processes run on the master device.

Views

System view

Predefined user roles

network-admin

Parameters

program-name: Specifies a process name, a case-insensitive string of 1 to 15 characters.

instance *instance-name*: Specifies the name of an instance of the specified process. The instance name is a case-insensitive string of 1 to 15 characters. If a process has only one instance, the system displays a prompt when you specify this option.

default: Configures the default placement policy for all processes.

Usage guidelines

You configure a process placement policy to optimize the distribution of processes in your system for optimal distribution of CPU and memory resources.

For an active process running only on the master device, it does not support placement optimization (by displaying a configuration failure prompt). When such an active process fails, the system automatically restarts the process. The standby processes are used for active/standby switchover and ISSU.

Some active processes can run on either the master or subordinate device. When such an active process fails, the system uses a placement policy to select a new active process among standby processes.

A process placement policy comprises the **affinity location-type**, **affinity location-set**, **affinity program**, and **affinity self** commands, which describe the preferences of the process for a specific location.

You can configure all the **affinity** commands in the placement policy for a process. Based on the placement policy and hardware resources, the system automatically determines the location for running the process. Before you apply the policy, you can use the **display placement reoptimize** command to view the predicted location for the process.

Examples

Enter the placement process view of BGP.

```
<Sysname> system-view
[Sysname] placement program bgp
[Sysname-program-bgp]
```

Enter the placement process view of BGP instance 100.

```
<Sysname> system-view
[Sysname] placement program bgp instance 100
[Sysname-program-bgp-100]
```

Enter default placement process view.

```
<Sysname> system-view
[Sysname] placement program default
[Sysname-program-default]
```

placement reoptimize

Use **placement reoptimize** to apply configured process placement policies for optimizing process placement.

Syntax

placement reoptimize

Views

System view

Predefined user roles

network-admin

Usage guidelines

After you issue this command, the system bases its placement decisions on the new process placement policies, hardware resources, and locations and states of active processes. If the new location for an active process is different from its current location, the system changes its state to standby and the state of the standby process on the new location to active. This active/standby switchover does not interrupt running services because no process is restarted.

To keep the system stable, HP recommends not performing any operation that requires process restart when you execute this command.

Examples

Reoptimize process placement.

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

[Sysname] placement reoptimize

Predicted changes to the placement

| Program | Current location | New location |
|---------|------------------|--------------|
| syslog | 1/0 | 1/0 |
| l3vpn | 1/0 | 1/0 |
| aaa | 1/0 | 1/0 |
| lauth | 1/0 | 1/0 |
| lsm | 1/0 | 1/0 |
| ip6addr | 1/0 | 1/0 |
| ip6base | 1/0 | 1/0 |
| rm | 1/0 | 1/0 |
| ipcfg | 1/0 | 1/0 |
| acl | 1/0 | 1/0 |
| tunnel | 1/0 | 1/0 |
| lagg | 1/0 | 1/0 |
| qos | 1/0 | 1/0 |
| ipcim | 1/0 | 1/0 |
| ipbase | 1/0 | 1/0 |
| eth | 1/0 | 1/0 |
| ipen | 1/0 | 1/0 |

Continue? [y/n]:y

Re-optimization of the placement start. You will be notified on completion

Re-optimization of the placement complete. Use 'display placement' to view the new placement

Index

[A](#) [B](#) [C](#) [D](#) [E](#) [M](#) [O](#) [P](#) [R](#) [S](#) [T](#) [V](#)

A

affinity location-set, [180](#)
affinity location-type, [181](#)
affinity program, [181](#)
affinity self, [182](#)

B

bfd authentication-mode, [156](#)
bfd demand enable, [157](#)
bfd detect-interface, [157](#)
bfd detect-multiplier, [158](#)
bfd echo enable, [159](#)
bfd echo-source-ip, [160](#)
bfd echo-source-ipv6, [160](#)
bfd min-echo-receive-interval, [161](#)
bfd min-receive-interval, [162](#)
bfd min-transmit-interval, [162](#)
bfd multi-hop authentication-mode, [163](#)
bfd multi-hop destination-port, [164](#)
bfd multi-hop detect-multiplier, [164](#)
bfd multi-hop min-receive-interval, [165](#)
bfd multi-hop min-transmit-interval, [166](#)
bfd session init-mode, [167](#)
bfd template, [167](#)

C

cfm ais enable, [32](#)
cfm ais level, [32](#)
cfm ais period, [33](#)
cfm ais-track link-status global, [34](#)
cfm ais-track link-status level, [34](#)
cfm ais-track link-status period, [35](#)
cfm ais-track link-status vlan, [36](#)
cfm cc enable, [37](#)
cfm cc interval, [38](#)
cfm dm one-way, [39](#)
cfm dm two-way, [39](#)
cfm enable, [40](#)
cfm linktrace, [41](#)

cfm linktrace auto-detection, [42](#)
cfm loopback, [43](#)
cfm md, [44](#)
cfm mep, [45](#)
cfm meplist, [46](#)
cfm mip-rule, [47](#)
cfm service-instance, [48](#)
cfm slm, [49](#)
cfm tst, [50](#)
control-vlan, [79](#)

D

display bfd session, [168](#)
display cfm ais, [51](#)
display cfm ais-track link-status, [53](#)
display cfm dm one-way history, [54](#)
display cfm linktrace-reply, [55](#)
display cfm linktrace-reply auto-detection, [57](#)
display cfm md, [58](#)
display cfm mep, [59](#)
display cfm meplist, [62](#)
display cfm mp, [62](#)
display cfm remote-mep, [64](#)
display cfm service-instance, [65](#)
display cfm status, [66](#)
display cfm tst, [66](#)
display dldp, [70](#)
display dldp statistics, [71](#)
display ha service-group, [183](#)
display monitor-link group, [109](#)
display oam, [1](#)
display oam configuration, [5](#)
display oam critical-event, [6](#)
display oam link-event, [7](#)
display placement location, [185](#)
display placement policy, [185](#)
display placement program, [186](#)
display placement reoptimize, [187](#)
display rrrp brief, [79](#)

- display rrp ring-group,82
- display rrp statistics,82
- display rrp verbose,85
- display smart-link flush,98
- display smart-link group,98
- display track,172
- display vrrp,114
- display vrrp ipv6,137
- display vrrp ipv6 statistics,144
- display vrrp statistics,121
- dldp authentication-mode,73
- dldp authentication-password,73
- dldp delaydown-timer,74
- dldp enable,75
- dldp global enable,76
- dldp interval,76
- dldp unidirectional-shutdown,77
- domain ring,88
- downlink up-delay,110

F

- fast-detection enable,89
- fast-edge-timer,90
- fast-timer,90
- flush enable,100

M

- monitor-link group,110

O

- oam enable,10
- oam errored-frame threshold,11
- oam errored-frame window,12
- oam errored-frame-period threshold,12
- oam errored-frame-period window,13
- oam errored-frame-seconds threshold,14
- oam errored-frame-seconds window,15
- oam errored-symbol-period threshold,16
- oam errored-symbol-period window,16
- oam global errored-frame threshold,17
- oam global errored-frame window,18
- oam global errored-frame-period threshold,19
- oam global errored-frame-period window,19
- oam global errored-frame-seconds threshold,20
- oam global errored-frame-seconds window,21
- oam global errored-symbol-period threshold,22

- oam global errored-symbol-period window,22
- oam global timer hello,23
- oam global timer keepalive,24
- oam mode,25
- oam remote-failure action,26
- oam remote-loopback,26
- oam remote-loopback interface,27
- oam remote-loopback reject-request,28
- oam timer hello,28
- oam timer keepalive,29

P

- placement program,188
- placement reoptimize,189
- port,111
- port,100
- port monitor-link group,112
- port smart-link group,101
- port smart-link group track,103
- preemption delay,104
- preemption mode,104
- protected-vlan,91
- protected-vlan,105

R

- reset bfd session statistics,170
- reset cfd dm one-way history,68
- reset cfd tst,68
- reset dldp statistics,78
- reset oam,30
- reset rrp statistics,92
- reset smart-link statistics,106
- reset vrrp ipv6 statistics,147
- reset vrrp statistics,124
- ring,93
- ring enable,94
- rrp domain,95
- rrp enable,96
- rrp ring-group,96

S

- smart-link flush enable,107
- smart-link group,107
- snmp-agent trap enable vrrp,125

T

- timer,97

track bfd, [174](#)
track cfd, [175](#)
track interface, [176](#)
track interface protocol, [177](#)
track nqa, [178](#)

V

vrrp check-ttl enable, [125](#)
vrrp dscp, [126](#)
vrrp ipv6 dscp, [147](#)
vrrp ipv6 mode, [148](#)
vrrp ipv6 vrid, [149](#)
vrrp ipv6 vrid preempt-mode, [150](#)
vrrp ipv6 vrid priority, [151](#)
vrrp ipv6 vrid shutdown, [151](#)
vrrp ipv6 vrid timer advertise, [152](#)
vrrp ipv6 vrid track, [153](#)
vrrp mode, [127](#)
vrrp version, [128](#)
vrrp vrid, [128](#)
vrrp vrid authentication-mode, [129](#)
vrrp vrid preempt-mode, [130](#)
vrrp vrid priority, [131](#)
vrrp vrid shutdown, [132](#)
vrrp vrid source-interface, [133](#)
vrrp vrid timer advertise, [134](#)
vrrp vrid track, [135](#)