Contents

BFD commands

Basic BFD commands

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 { **hmac-md5** | **hmac-mmd5** | **hmac-msha1** | **hmac-sha1** | **m-md5** | **m-sha1** | **md5** | **sha1** | **simple** } *key-id* { **cipher** | **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

hmac-md5: Specifies the HMAC MD5 algorithm.

hmac-mmd5: Specifies the HMAC Meticulous MD5 algorithm.

hmac-msha1: Specifies the HMAC Meticulous SHA1 algorithm.

hmac-sha1: Specifies the HMAC SHA1 algorithm.

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: Specifies a key in encrypted form.

plain: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its encrypted form is a case-sensitive string of 33 to 53 characters.

Usage guidelines

Use this command to enhance BFD session security.

BFD version 0 does not support this command. The configuration does not take effect.

Examples

Configure VLAN-interface 11 to perform simple authentication for single-hop BFD control packets, setting the authentication key ID to **1** and plaintext key to **123456**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] bfd authentication-mode simple 1 plain 123456
```

bfd dampening

Use **bfd dampening** to configure BFD session flapping suppression.

Use **undo bfd dampening** to disable BFD session flapping suppression.

Syntax

bfd dampening [**maximum** *maximum-interval* **initial** *initial-interval* **secondary** *secondary-interval*]

undo bfd dampening

Default

BFD sessions are not suppressed.

Views

System view

Predefined user roles

network-admin

Parameters

maximum-interval: Specifies the maximum amount of time a BFD session is suppressed, in the range of 1 to 3600 seconds. The default is 20 seconds.

initial-interval: Specifies the amount of time a BFD session is suppressed for the first time. The value range for the *initial-interval* argument is 1 to 3600 seconds. The default is 6 seconds.

secondary-interval: Specifies the amount of time a BFD session is suppressed for the second time. The value range for the *secondary-interval* argument is 1 to 3600 seconds. The default is 10 seconds.

Usage guidelines

When BFD detects a link failure, it tears down the BFD session and notifies the upper-layer protocol of the failure. When the upper-layer protocol re-establishes a neighbor relationship, the BFD session comes up again. BFD session flaps occur when a link fails and recovers repeatedly, which consumes significant system resources and causes network instability.

This command allows you to suppress BFD session flapping by using the *initial-interval*, *secondary-interval*, and *maximum-interval* arguments.

- A BFD session is suppressed within the specified interval. The suppression time does not exceed the *maximum-interval*.
- After a BFD session goes down for the second time, it cannot be re-established within the *initial-interval*.
- After a BFD session goes down for the third time, it cannot be re-established within the *secondary-interval*.

- After a BFD session goes down for the fourth time and at any later time, the following rules apply:
  - If *secondary-interval* × 2^{n-3} is smaller than or equal to the *maximum-interval*, the BFD session cannot be re-established within the *secondary-interval* × 2^{n-3}.
  - If *secondary-interval* × 2^{n-3} is greater than the *maximum-interval*, the BFD session cannot be re-established within the *maximum-interval*.

  The letter n, starting from 4, is the number of times the BFD session flaps.

Examples

Enable BFD session flapping suppression, and set the *maximum-interval*, *initial-interval*, and *secondary-interval* to 12 seconds, 4 seconds, and 8 seconds, respectively.

```
<Sysname> system-view
[Sysname] bfd dampening maximum 12 initial 4 secondary 8
```

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 with 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.

BFD version 0 does not support this command. The configuration does not take effect.

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* [**discriminator local** *local-value* **remote** *remote-value*] [**template** *template-name*]

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.

discriminator: Specifies BFD session discriminators. If you do not specify discriminators, the device obtains BFD session discriminators through autonegotiation.

local *local-value*: Specifies the local discriminator. The value range for the *local-value* argument is 97 to 128.

remote *remote-value*: Specifies the remote discriminator in the range of 1 to 4294967295.

template *template-name*: Specifies a template by its name, a case-sensitive string of 1 to 63 characters. If you do not specify a template, the BFD session uses the BFD parameters configured in interface view.

Usage guidelines

This command implements fast collaboration between interface state and BFD session state. When BFD detects a link fault, it sets the link layer protocol state to DOWN(BFD). This behavior helps applications relying on the link layer protocol state achieve fast convergence.

The source IP address of control packets is specified manually, and the destination IP address is fixed at 224.0.0.184. As a best practice, specify the IP address of the interface as the source IP address. If the interface does not have an IP address, specify a unicast IP address other than 0.0.0.0 as the source IP address.

You can associate the state of the following interfaces with BFD:

- Layer 2 Ethernet interfaces.
- Member ports in a Layer 2 aggregation group.
- Layer 3 Ethernet interfaces.
- Member ports in a Layer 3 aggregation group.
- Layer 3 Ethernet subinterfaces.
- VLAN interfaces.
- Layer 2 aggregate interfaces.
- Layer 3 aggregate interfaces.
- Layer 3 aggregate subinterfaces.

This command must be executed on both ends of the link for a BFD session to be established.

If you execute both the **bfd detect-interface** and **bfd echo enable** commands for an interface, only the **bfd detect-interface** command takes effect.

For BFD detection to take effect, do not execute this command on both a Layer 3 Ethernet interface and its subinterface.

For BFD detection to take effect, do not execute this command on both a Layer 2 Ethernet interface and the VLAN interface created for the VLAN to which the Layer 2 Ethernet interface is assigned.

For BFD detection to take effect, do not execute this command on the following interfaces at the same time:

- A Layer 3 aggregate interface.
- A subinterface of the Layer 3 aggregate interface.
- A member port of the Layer 3 aggregate interface.

For BFD detection to take effect, do not execute this command on the following interfaces at the same time:

- A Layer 2 aggregate interface.
- A member port of the Layer 2 aggregate interface.
- The VLAN interface to which the Layer 2 aggregate interface belongs.

If the peer device does not support obtaining BFD session discriminators through autonegotiation, you must specify the discriminators on both the local and peer devices. Without the discriminators, the BFD session cannot come up.

The BFD session discriminators must match on the local and peer devices. For example, if you configure **bfd detect-interface source-ip** 20.1.1.1 **discriminator local** 513 **remote** 514 on the local device, you must configure **bfd detect-interface source-ip** 20.1.1.2 **discriminator local** 514 **remote** 513 on the peer device.

The local discriminators of BFD sessions for interfaces on the same device must be different.

Examples

Create a BFD session to detect the state of VLAN-interface 10, and specify the source IP address as 20.1.1.1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] bfd detect-interface source-ip 20.1.1.1
```

bfd detect-multiplier

Use **bfd detect-multiplier** to set the single-hop detection time multiplier for control packet mode and the detection time multiplier for echo packet mode.

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 for control packet mode and the detection time multiplier for echo packet mode are both 5.

Views

Interface view

BFD template view

Predefined user roles

network-admin

Parameters

value: Specifies a detection time multiplier. The value range for this argument is 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 1 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

Set the single-hop detection time multiplier for control packet mode and the detection time multiplier for echo packet mode to 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 disable the echo packet mode.

Syntax

bfd echo [**receive** | **send**] **enable**

undo bfd echo [**receive** | **send**] **enable**

Default

The echo packet mode is disabled.

Views

Interface view

Predefined user roles

network-admin

Parameters

receive: Specifies the echo packet receiving capability.

send: Specifies the echo packet sending capability.

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 performs the following operations:

- Periodically sends echo packets to detect link connectivity.
- Decreases the control packet receiving rate at the same time.

To enable only the echo packet receiving capability, use the **bfd echo receive enable** command.

To enable only the echo packet sending capability, use the **bfd echo send enable** command.

If you do not specify the **receive** or **send** keyword, the command enables both the echo packet receiving and sending capabilities.

If you configure both the **bfd detect-interface** and **bfd echo enable** commands for an interface, only the **bfd detect-interface** command takes effect.

BFD version 0 does not support this command. The configuration does not take effect.

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 set 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 *interval*

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

interval: Specifies the 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.

The local end stops sending echo packets after autonegotiation with the remote end if the following conditions are met:

- The echo packet mode is enabled on the local end.
- The minimum interval for receiving BFD echo packets is set to 0 milliseconds on the remote end.

Examples

Set the minimum interval for receiving BFD echo packets to 500 milliseconds on VLAN-interface 11.

```
<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 set 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 *interval*

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

interval: Specifies the minimum interval for receiving single-hop BFD control packets, in milliseconds. The value range for this argument is 3 to 1000.

Usage guidelines

Use 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 following values:

- Minimum interval for transmitting BFD control packets on the peer end.
- Minimum interval for receiving BFD control packets on the local end.

Examples

Set the minimum interval for receiving single-hop BFD control packets to 500 milliseconds on VLAN-interface 11.

```
<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 set 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 *interval*

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

interval: Specifies the minimum interval for transmitting single-hop BFD control packets, in milliseconds. The value range for this argument is 3 to 1000.

Usage guidelines

Use this command to prevent the BFD packet sending rate from exceeding the device capability.

The actual BFD control packet transmitting interval on the local end is the greater value between the following values:

- Minimum interval for transmitting BFD control packets on the local end.
- Minimum interval for receiving BFD control packets on the peer end.

Examples

Set the minimum interval for transmitting single-hop BFD control packets to 500 milliseconds on VLAN-interface 11.

```
<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 { **hmac-md5** | **hmac-mmd5** | **hmac-msha1** | **hmac-sha1** | **m-md5** | **m-sha1** | **md5** | **sha1** | **simple** } *key-id* { **cipher** | **plain** } *string*

undo bfd multi-hop authentication-mode

Default

No authentication is performed.

Views

System view

Predefined user roles

network-admin

Parameters

hmac-md5: Specifies the HMAC MD5 algorithm.

hmac-mmd5: Specifies the HMAC Meticulous MD5 algorithm.

hmac-msha1: Specifies the HMAC Meticulous SHA1 algorithm.

hmac-sha1: Specifies the HMAC SHA1 algorithm.

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: Specifies a key in encrypted form.

plain: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the key. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its encrypted form is a case-sensitive string of 33 to 53 characters.

Usage guidelines

Use this command to enhance BFD session security.

BFD version 0 does not support this command. The configuration does not take effect.

Examples

Configure the simple authentication mode for multihop BFD control packets, setting the authentication key ID to 1 and key 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

Specify 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 set the multihop detection time multiplier for control packet mode.

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 for control packet mode 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 2 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

Mode	Detection interval
Control packet mode BFD session in demand mode	Detection time multiplier of the sender × actual packet sending interval of the sender

Examples

Set the multihop detection time multiplier to 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 set 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 *interval*

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

interval: Specifies the minimum interval for receiving multihop BFD control packets, in milliseconds. The value range for this argument is 3 to 1000.

Usage guidelines

Use this command to prevent the packet sending rate of the peer end from exceeding the packet receiving capability (minimum control packet receiving interval) of the local end. If the receiving capability is exceeded, the peer end dynamically adjusts the BFD control packet sending interval to the minimum control packet receiving interval of the local end.

Examples

Set the minimum interval for receiving multihop BFD control packets to 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 set 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 *interval*

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

interval: Specifies the minimum interval for transmitting multihop BFD control packets, in milliseconds. The value range for this argument is 3 to 1000.

Usage guidelines

Use this command to prevent the BFD packet sending rate from exceeding the device capability.

The actual BFD control packet transmitting interval on the local end is the greater value between the following values:

- Minimum interval for transmitting BFD control packets on the local end.
- Minimum interval for receiving BFD control packets on the peer end.

Examples

Set the minimum interval for transmitting multihop BFD control packets to 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: Specifies 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: Specifies 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

A minimum of one end must operate in active mode for a BFD session to be established.

BFD version 0 does not support this command. The configuration does not take effect.

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 its view, or enter the view of an existing BFD template.

Use **undo bfd template** to delete the BFD template.

Syntax

bfd template *template-name*

undo bfd template *template-name*

Default

No BFD templates exist.

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 brief information about all IPv4 BFD sessions.

```
<Sysname> display bfd session

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 session working in control packet mode:

 LD/RD          SourceAddr      DestAddr        State    Holdtime    Interface
 513/513        1.1.1.1         1.1.1.2         Up       2297ms      Vlan100
```

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 in control packet mode:

       Local Discr: 513                 Remote Discr: 513
         Source IP: 1.1.1.1           Destination IP: 1.1.1.2
     Session State: Up                      Interface: Vlan-interface100
      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: 0
          Protocol: OSPF
          Version:1
         Diag Info: No Diagnostic
```

Display brief information about all IPv6 BFD sessions.

```
<Sysname> display bfd session

 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv6 session working in control packet 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: Vlan100
         Hold Time: 2142ms
```

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 in control packet 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: Vlan-interface100
      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: 0
          Protocol: OSPFv3
          Version:1
         Diag Info: No Diagnostic
```

Table 3 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.
IPv4 session working in control packet mode	BFD session type and operating mode: • **IPv4 session working in control packet mode**. • **IPv4 session working in echo mode**. • **IPv6 session working in control packet mode**. • **IPv6 session working in echo mode**.
Local Discr/LD	Local discriminator of the session.
Remote Discr/RD	Remote discriminator 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: **Down**, **Init**, or **Up**.
Interface	Name of the interface of the session.
Min Tx Inter	Minimum BFD packet transmission interval.
Min Rx Inter	Minimum BFD packet receiving interval.
Act Tx Inter	Actual BFD packet transmission 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 the session detection timer expires, in milliseconds.

Field	Description
	For a BFD session in **Down** state, this field displays **0ms**.
Auth mode	Session authentication mode.
Connect Type	Connection type of the interface: Direct or indirect.
Running up for	Time period for which the session has been up.
Detect Mode	Detection mode: • **Async**—Asynchronous mode. • **Demand**—Demand mode. • **Async/Echo**—Asynchronous mode with echo detection enabled. • **Demand/Echo**—Demand mode with echo detection enabled.
Slot	Slot number.
Diag Info	Diagnostic information about the session: • **No Diagnostic**. • **Control Detection Time Expired**—A control packet mode BFD session goes down because local detection times out. • **Echo Function Failed**—An echo packet mode BFD session goes down, because local detection times out or the source IP address of echo packets is deleted. • **Neighbor Signaled Session Down**—The remote end notifies the local end of BFD session down. • **Administratively Down**—The local system prevents a BFD session from being established.

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
```

snmp-agent trap enable bfd

Use **snmp-agent trap enable bfd** to enable SNMP notifications for BFD.

Use **undo snmp-agent trap enable bfd** to disable SNMP notifications for BFD.

Syntax

snmp-agent trap enable bfd

undo snmp-agent trap enable bfd

Default

All SNMP notifications are enabled for BFD.

Views

System view

Predefined user roles

network-admin

Usage guidelines

To report critical BFD events to an NMS, enable SNMP notifications for BFD. For BFD event notifications to be sent correctly, you must also configure SNMP as described in the network management and monitoring configuration guide for the device.

Examples

Disable SNMP notifications for BFD.

```
<Sysname> system-view
[Sysname] undo snmp-agent trap enable bfd
```