Contents

RSVP commands

authentication challenge

Use **authentication challenge** to enable the RSVP challenge-response handshake feature globally or for an RSVP neighbor.

Use **undo authentication challenge** to disable the challenge-response handshake feature globally or for an RSVP neighbor.

Syntax

authentication challenge

undo authentication challenge

Default

The RSVP challenge-response handshake feature is disabled.

Views

RSVP view

RSVP neighbor view

Predefined user roles

network-admin

mdc-admin

Usage guidelines

To prevent packet replay attacks, RSVP requires received authentication messages to carry incremental sequence numbers. To verify the subsequent messages, RSVP saves the sequence number of the last valid message in a receive-type security association.

However, when RSVP creates a new receive-type security association, it cannot obtain the sequence number of the sender. To successfully establish the receive-type security association, RSVP sets the receive sequence number to 0 by default. Then, the association can receive a message with any sequence number from the peer. Because this introduces a vulnerability to replay attacks, you should execute the **authentication challenge** command. When RSVP creates a receive-type security association, it will perform a challenge-response handshake to obtain the sequence number of the sender.

RSVP challenge-response handshake can be configured in the following views:

- **RSVP view**—Configuration applies to all RSVP security associations.
- **RSVP neighbor view**—Configuration applies only to RSVP security associations with the specified neighbor.
- **Interface view**—Configuration applies only to RSVP security associations established on the current interface.

The execution of this command affects only security associations established after the execution. To apply the setting to existing security associations, you must execute the **reset rsvp authentication** command to delete and then re-establish the security associations.

Examples

Enable RSVP challenge-response handshake globally.

```
<Sysname> system-view
[Sysname] rsvp
```

```
[Sysname-rsvp] authentication challenge
```

Enable challenge-response handshake for RSVP neighbor 1.1.1.9.

```
<Sysname> system-view
[Sysname] rsvp
[Sysname-rsvp] peer 1.1.1.9
[Sysname-rsvp-peer-1.1.1.9] authentication challenge
```

Related commands

authentication key

authentication lifetime

authentication window-size

display rsvp authentication

reset rsvp authentication

rsvp authentication challenge

rsvp authentication key

rsvp authentication lifetime

rsvp authentication window-size

authentication key

Use **authentication key** to enable RSVP authentication globally or for an RSVP neighbor, and configure the authentication key.

Use **undo authentication key** to disable RSVP authentication.

Syntax

authentication key { **cipher** | **plain** } *string*

undo authentication key

Default

RSVP authentication is disabled.

Views

RSVP view

RSVP neighbor view

Predefined user roles

network-admin

mdc-admin

Parameters

cipher: Specifies an authentication key in encrypted form.

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

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

Usage guidelines

RSVP authentication ensures integrity of RSVP messages, and prevents false resource reservation requests from occupying network resources.

With RSVP authentication, the sender uses the MD5 algorithm and the authentication key to calculate a message digest for an RSVP message. The sender inserts the message digest to the RSVP message. When the receiver receives the message, it performs the same calculation and compares the result with the message digest received. If the two digests match, the receiver accepts the message. If the two digests do not match, it drops the message.

RSVP authentication can be configured in the following views:

- **RSVP view**—Configuration applies to all RSVP security associations.
- **RSVP neighbor view**—Configuration applies only to RSVP security associations with the specified RSVP neighbor.
- **Interface view**—Configuration applies only to RSVP security associations established on the current interface.

Configurations in RSVP neighbor view, interface view, and RSVP view are in descending order of priority. If RSVP authentication for a neighbor is enabled in both RSVP neighbor view and RSVP view with different authentication keys configured, the key configured in RSVP neighbor view is used.

To re-establish a security association, you must delete the authentication key used by the current security association or delete the current security association (using the **reset rsvp authentication** command). Then, the device can re-establish a security association by looking up a new authentication key in order of priorities.

After you enable RSVP authentication on the local device, you must also enable RSVP authentication and configure the same authentication key on the RSVP neighbor.

Examples

Enable RSVP authentication globally, and configure the authentication key as a plaintext string of **abcdefgh**.

```
<Sysname> system-view
[Sysname] rsvp
[Sysname-rsvp] authentication key plain abcdefgh
```

Enable RSVP authentication for neighbor 1.1.1.9, and configure the authentication key as a plaintext string of **abcdefgh**.

```
<Sysname> system-view
[Sysname] rsvp
[Sysname-rsvp] peer 1.1.1.9
[Sysname-rsvp-peer-1.1.1.9] authentication key plain abcdefgh
```

Related commands

authentication challenge

authentication lifetime

authentication window-size

display rsvp authentication

reset rsvp authentication

rsvp authentication challenge

rsvp authentication key

rsvp authentication lifetime

rsvp authentication window-size

authentication lifetime

Use **authentication lifetime** in RSVP view to set the global idle timeout for RSVP security associations.

Use **authentication lifetime** in RSVP neighbor view to set the idle timeout for RSVP security associations with an RSVP neighbor.

Use **undo authentication lifetime** to restore the default.

Syntax

authentication lifetime *life-time*

undo authentication lifetime

Default

The idle timeout for an RSVP security association is 1800 seconds.

Views

RSVP view

RSVP neighbor view

Predefined user roles

network-admin

mdc-admin

Parameters

life-time: Specifies the RSVP security association idle timeout in the range of 30 to 86400 seconds.

Usage guidelines

When RSVP authentication is enabled, the device dynamically establishes security associations when receiving and sending RSVP messages.

To release memory resources, each security association has an idle timeout. When a security association is idle for the specified timeout time, the device deletes the security association. When the device sends or receives an authenticated RSVP message, it resets the idle timeout timer for the corresponding security association.

The RSVP authentication idle timeout can be configured in the following views:

- **RSVP view**—Configuration applies to all RSVP security associations.
- **RSVP neighbor view**—Configuration applies only to RSVP security associations with the specified RSVP neighbor.
- **Interface view**—Configuration applies only to RSVP security associations established on the current interface.

An RSVP security association established by using the authentication key configured in a view uses the idle timeout configured in the same view.

A modification to the idle timeout affects only security associations established after the modification. To apply the new setting to existing security associations, you must execute the **reset rsvp authentication** command to delete and then re-establish the security associations.

Examples

Set the global idle timeout to 100 seconds for RSVP security associations.

```
<Sysname> system-view
[Sysname] rsvp
```

```
[Sysname-rsvp] authentication lifetime 100
```

Set the idle timeout to 100 seconds for the security associations with RSVP neighbor 1.1.1.9.

```
<Sysname> system-view
[Sysname] rsvp
[Sysname-rsvp] peer 1.1.1.9
[Sysname-rsvp-peer-1.1.1.9] authentication lifetime 100
```

Related commands

authentication challenge

authentication key

authentication window-size

display rsvp authentication

reset rsvp authentication

rsvp authentication challenge

rsvp authentication key

rsvp authentication lifetime

rsvp authentication window-size

authentication window-size

Use **authentication window-size** in RSVP view to set the global RSVP authentication window size, which is the maximum number of authenticated RSVP messages that can be received out of sequence.

Use **authentication window-size** in RSVP neighbor view to set the RSVP authentication window size for an RSVP neighbor.

Use **undo authentication window-size** to restore the default.

Syntax

authentication window-size *number*

undo authentication window-size

Default

Only one authenticated RSVP message can be received out of sequence.

Views

RSVP view

RSVP neighbor view

Predefined user roles

network-admin

mdc-admin

Parameters

number: Specifies the maximum number of authenticated RSVP messages that can be received out of sequence, in the range of 1 to 64.

Usage guidelines

To protect against replay attacks, the sender places a unique sequence number in each RSVP message that contains authentication information. The sender increases the value of the sequence number by one each time it sends an RSVP message. If the sequence number of a received message is in the specified authentication window size, the receiver accepts the message. If it is not in the specified authentication window size, the receiver discards the message.

When the receiver receives an RSVP message, it compares the sequence number of the last accepted RSVP message with the sequence number of the newly received RSVP message.

- If the new sequence number is greater than the last sequence number, RSVP accepts the message and updates the last sequence number with the new sequence number.
- If the new sequence number equals the last sequence number, RSVP regards the message a replay message and discards the message.
- If the new sequence number is smaller than the last sequence number but greater than the last sequence number minus the window size, and has never been received before, RSVP accepts the message. If the new sequence number has been received before, RSVP regards the message a replay message and discards the message.
- If the new sequence number is smaller than or equal to the last sequence number minus the window size, RSVP regards the message invalid and discards the message.

By default, the authentication window size is 1. If the sequence number of a newly received RSVP message is smaller than that of the last accepted message, the device discards the message. However, if the sender sends multiple RSVP messages in a short time, these messages might arrive at the neighbor out of sequence. If you use the default window size, the out-of-sequence messages will be discarded. To solve this problem, you can use the **authentication window-size** command to configure a correct window size.

A security association established by using the authentication key configured in a view uses the window size configured in that view.

A modification to the window size affects only security associations established after the modification. To apply the new setting to existing security associations, you must execute the **reset rsvp authentication** command to delete and then re-establish the security associations.

Examples

In RSVP view, set the maximum number of out-of-sequence authenticated RSVP messages that can be received to 10.

```
<Sysname> system-view
[Sysname] rsvp
[Sysname-rsvp] authentication window-size 10
```

In RSVP neighbor view, set the maximum number of out-of-sequence authenticated RSVP messages that can be received from RSVP neighbor 1.1.1.9 to 10.

```
<Sysname> system-view
[Sysname] rsvp
[Sysname-rsvp] peer 1.1.1.9
[Sysname-rsvp-peer-1.1.1.9] authentication window-size 10
```

Related commands

authentication challenge

authentication key

authentication lifetime

display rsvp authentication

reset rsvp authentication

rsvp authentication challenge

rsvp authentication key

rsvp authentication lifetime

rsvp authentication window-size

display rsvp

Use **display rsvp** to display RSVP information.

Syntax

display rsvp [**interface** [*interface-type interface-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

interface: Displays RSVP information on interfaces. If you do not specify this keyword, the command displays global RSVP information.

interface-type interface-number: Displays RSVP information on the interface specified by its type and number. If you specify the **interface** keyword without this argument, the command displays RSVP information for all interfaces.

Examples

Display global RSVP information.

```
<Sysname> display rsvp
LSR ID: 50.0.0.1                      Fast Reroute time: 300 sec
Refresh interval: 30 sec              Keep multiplier: 3
Hello interval: 3 sec                 Hello lost: 4
Graceful Restart: Disabled            DSCP value: 48
Authentication: Enabled
  Lifetime: 300 sec
  Window size: 64
  Challenge: Enabled
P2P statistics:
  PSB number: 5                       RSB number: 5
  LSP number: 5                       Request number: 5
  Peer number: 5                      SA number: 5
P2MP statistics:
  PSB number: 0                       RSB number: 0
  LSP number: 0                       Request number: 0
  Peer number: 0                      SA number: 0
```

Table 1 Command output

Field	Description
Fast Reroute time	Interval for detecting whether a better bypass CRLSP is available for a primary CRLSP, in seconds.
Refresh interval	Interval for refreshing Path and Resv messages, in seconds.
Keep multiplier	PSB and RSB timeout multiplier.
Hello interval	Interval for sending hello requests, in seconds.
Hello lost	Maximum number of consecutive lost or erroneous hellos allowed.
DSCP value	DSCP value for outgoing RSVP packets.
Authentication	RSVP authentication state.
Lifetime	Idle timeout for RSVP security associations, in seconds.
Window size	Maximum number of out-of-sequence authenticated RSVP messages that can be received.
Challenge	State of the challenge-response handshake feature.
P2P statistics	RSVP P2P statistics.
PSB number	Total number of PSBs.
RSB number	Total number of RSBs.
LSP number	Total number of LSPs established by RSVP.
Request number	Total number of RSVP request data blocks.
Peer number	Total number of RSVP neighbors.
SA number	Total number of security associations.
P2MP statistics	This field is not supported in the current software version. RSVP P2MP statistics.

Display RSVP information for all interfaces.

```
<Sysname> display rsvp interface
Interface: Vlan10                       Logical interface handle: 0x19a5
State: Up                               IP address: 50.1.0.1
MPLS TE: Enabled                        RSVP: Enabled
Hello: Enabled                          BFD: Enabled
Summary refresh: Enabled                Reliability: Disabled
Retransmit interval: 500 ms             Retransmit increment: 1
Authentication: Enabled
  Lifetime: 300 sec
  Window size: 64
  Challenge: Enabled
Bypass tunnels: Tunnel1

Interface: Vlan20                       Logical interface handle: 0x19a6
State: Up                               IP address: 50.2.0.1
MPLS TE: Enabled                        RSVP: Enabled
Hello: Enabled                          BFD: Enabled
Summary refresh: Disabled               Reliability: Disabled
Retransmit interval: 500 ms             Retransmit increment: 1
```

```
Authentication: Enabled
  Lifetime: 300 sec
  Window size: 64
  Challenge: Enabled
Bypass tunnels: Tunnel1, Tunnel2, Tunnel3
```

Table 2 Command output

Field	Description
Logical interface handle	Logical interface handle, used to distinguish logical outgoing interfaces on the RSVP interface.
State	Interface state recorded by RSVP: **UP** or **Down**.
IP address	IP address of the current interface used by RSVP.
MPLS TE	MPLS TE state on the interface.
RSVP	RSVP state on the interface.
Hello	State of the hello extension feature on the interface.
BFD	BFD state on the interface.
Summary refresh	State of the summary refresh feature on the interface.
Reliability	State of the reliable RSVP message delivery feature on the interface.
Retransmit interval	Initial retransmission interval for reliable RSVP message delivery, in milliseconds.
Retransmit increment	Retransmission increment value for reliable RSVP message delivery.
Authentication	RSVP authentication state on the interface.
Lifetime	Idle timeout for RSVP security associations, in seconds.
Window size	Maximum number of out-of-sequence authenticated RSVP messages that can be received.
Challenge	State of the challenge-response handshake feature on the interface.
Bypass tunnels	Bypass tunnels configured on the interface for fast reroute (FRR). If no bypass tunnels are configured, this field displays **None**.

display rsvp authentication

Use **display rsvp authentication** to display information about the security associations established with RSVP neighbors.

Syntax

display rsvp authentication [**from** *ip-address*] [**to** *ip-address*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

from *ip-address*: Displays information about the security associations with the specified source IP address.

to *ip-address*: Displays information about the security associations with the specified destination IP address.

verbose: Displays detailed information about RSVP security associations. If you do not specify this keyword, the command displays brief information about RSVP security associations.

Usage guidelines

After RSVP authentication is enabled, the device automatically establishes security associations when sending and receiving RSVP messages. A security association includes the following information:

- IP address of the authentication source node.
- IP address of the authentication destination node.
- Authentication direction.
- Authentication type.
- Authentication key.
- Authentication expiration time.

The device obtains the RSVP authentication source and destination IP addresses from the IP header or RSVP message objects, as shown in Table 3.

Table 3 How to get RSVP authentication source and destination IP addresses

Message type received or sent	Authentication source IP	Authentication destination IP
Path	Address in the HOP object of the RSVP message.	Address in the SESSION object of the RSVP message.
PathTear	Address in the HOP object of the RSVP message.	Address in the SESSION object of the RSVP message.
PathError	Source IP address in the IP header	Destination IP address in the IP header
Resv	Address in the HOP object of the RSVP message.	Destination IP address in the IP header
ResvTear	Address in the HOP object of the RSVP message.	Destination IP address in the IP header
ResvError	Address in the HOP object of the RSVP message.	Destination IP address in the IP header
ResvConfirm	Source IP address in the IP header	Address in the CONFIRM object of the RSVP message.
ACK	Source IP address in the IP header	Destination IP address in the IP header
Srefresh	Source IP address in the IP header	Destination IP address in the IP header
Hello	Source IP address in the IP header	Destination IP address in the IP header

If you do not specify the **from** *ip-address* **to** *ip-address* options, this command displays information about the security associations established with all RSVP neighbors.

Examples

Display brief information about the security associations established with all RSVP neighbors.

```
<Sysname> display rsvp authentication
```

```
From            To              Mode    Type      Key-ID       Expiration
57.10.10.1      57.10.10.2      Receive Interface 000103000000 280s
57.10.10.2      57.10.10.1      Send    Interface 000103000000 280s
```

Table 4 Command output

Field	Description
From	RSVP authentication source IP address.
To	RSVP authentication destination IP address.
Mode	Direction of the security association: • **Receive**—Receive security association, used to authenticate messages received from an RSVP neighbor. • **Send**—Send security association, used to authenticate messages sent to an RSVP neighbor.
Type	Type of the security association: • **Peer**—Security association established in RSVP neighbor view. • **Interface**—Security association established in interface view. • **Global**—Security association established in RSVP view.
Key-ID	Key ID of the security association. • For a send security association, this field displays the local key ID. • For a receive security association, this field displays the key ID received from the peer.
Expiration	Idle timeout remaining time of the security association, in seconds.

Display detailed information about the security associations established with all RSVP neighbors.

```
<Sysname> display rsvp authentication verbose
From: 20.1.1.1                          To: 4.4.4.9
Mode: Send                              Type: Interface
Challenge: Supported                    Peer: 20.1.1.2
Local key ID: 0x000104000000            Peer key ID: 0x0
Lifetime: 1800 sec                      Expiration time: 1781 sec
Window size: 1
Last sent sequence number:
  5781735195480686593

From: 20.1.1.2                          To: 20.1.1.1
Mode: Receive                           Type: Interface
Challenge: Not configured               Peer: 20.1.1.2
Local key ID: 0x0                       Peer key ID: 0x000104000000
Lifetime: 1800 sec                      Expiration time: 1798 sec
Window size: 1
Received sequence numbers:
  5781742445385482241
```

Table 5 Command output

Field	Description
From	RSVP authentication source IP address.
To	RSVP authentication destination IP address.

Field	Description
Mode	Direction of the security association: • **Receive**—Receive security association, used to authenticate messages received from an RSVP neighbor. • **Send**—Send security association, used to authenticate messages sent to an RSVP neighbor.
Type	Type of the security association: • **Peer**—Security association established in RSVP neighbor view. • **Interface**—Security association established in interface view. • **Global**—Security association established in RSVP view.

Challenge	State of the authentication challenge-response feature:
	• **Not configured**—The challenge-response handshake feature is disabled locally. (For a receive security association.)
	• **Configured**—The challenge-response handshake feature is enabled locally. (For a receive security association.)
	• **In progress**—The local device has sent an Integrity Challenge message to the peer and is waiting for the Integrity Response message from the peer.
	• **Completed**—The local device has received an Integrity Response message from the peer and the message has passed the authentication.
	• **Failed**—The **Failed** state is displayed when one of the following events occurs:
	  ○ The local device has received an Integrity Response message from the peer but the message failed the authentication.
	  ○ The local device has not received any valid Integrity Response after sending three Integrity Challenge messages to the peer.
	  ○ The challenge-response feature is disabled on the peer.
	• **Supported**—The local device supports the challenge-response feature. (For a send security association.)

Peer	IP address of the authentication neighbor.
Local key ID	Local key ID, for a send security association.
Peer key ID	Peer key ID, for a receive security association.
Lifetime	Idle timeout of the security association, in seconds.
Expiration time	Idle timeout remaining time of the security association, in seconds.
Window size	Maximum number of out-of-sequence authenticated RSVP messages that can be received.
Received sequence numbers	Sequence numbers of the received messages. This field can display the sequence numbers for a maximum of *window-size* messages.
Last sent sequence number	Sequence number of the last sent message.

Related commands

`authentication challenge`

`authentication key`

`authentication lifetime`

`authentication window-size`

`reset rsvp authentication`

`rsvp authentication challenge`

`rsvp authentication key`

rsvp authentication lifetime

rsvp authentication window-size

display rsvp lsp

Use **display rsvp lsp** to display information about CRLSPs established by RSVP.

Syntax

display rsvp lsp [**destination** *ip-address*] [**source** *ip-address*] [**tunnel-id** *tunnel-id*] [**lsp-id** *lsp-id*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

destination *ip-address*: Displays information about the CRLSP with the specified tunnel destination address.

source *ip-address*: Displays information about the CRLSP with the specified tunnel source address. The tunnel source address is the extended tunnel ID in the Session object of an RSVP message.

tunnel-id *tunnel-id*: Displays information about the CRLSP with the specified tunnel ID in the range of 0 to 65535.

lsp-id *lsp-id*: Displays information about the CRLSP with the specified LSP ID in the range of 0 to 65535.

verbose: Displays detailed information about CRLSPs. If you do not specify this keyword, the command displays brief information about CRLSPs.

Usage guidelines

If you do not specify any parameters, this command displays brief information about all CRLSPs established by RSVP.

Examples

Display brief information about all CRLSPs established by RSVP.

```
<Sysname> display rsvp lsp
Destination     Source          Tunnel-ID LSP-ID Direction  Tunnel-name
50.0.0.1        50.0.0.3        1         1      Uni        Sysname_t0
50.0.0.1        50.0.0.3        2         2      Bi-Down    Sysname_t1
```

Table 6 Command output

Field	Description
Destination	Tunnel destination address.
Source	Tunnel source address.

Field	Description
Direction	Tunnel direction: • **Uni**—Unidirectional tunnel. • **Bi-Down**—Forward CRLSP of a bidirectional tunnel. • **Bi-Up**—Backward CRLSP of a bidirectional tunnel.
Tunnel-name	Tunnel name. The tunnel ingress node generates the name and notifies other nodes of the name through a Path message. When the ingress node is an H3C device, the tunnel name is *Sysname*_t*tunnel-ID*, where *Sysname* represents the device name, and *tunnel-ID* represents the ID of the tunnel. You can configure the device name by executing the **sysname** command in system view. This field contains a maximum of 80 characters, and displays the first 77 characters and three dots (.) if the name contains more than 80 characters.

Display detailed information about all CRLSPs established by RSVP.

```
<Sysname> display rsvp lsp verbose
Tunnel name: Sysname_t1
Destination: 3.3.3.9                    Source: 1.1.1.9
Tunnel ID: 1                            LSP ID: 5
LSR type: Transit                       Direction: Unidirectional
Setup priority: 7                       Holding priority: 7
In-Label: 1146                          Out-Label: 3
In-Interface: Vlan10                    Out-Interface: Vlan20
Nexthop: 57.20.20.1                     Exclude-any: 0
Include-Any: 0                          Include-all: 0
Mean rate (CIR): 0.00 kbps              Mean burst size (CBS): 1000.00 bytes
Path MTU: 1500                          Class type: CT0
RRO number: 8
  57.10.10.1/32      Flag: 0x00 (No FRR)
  57.10.10.2/32      Flag: 0x40 (No FRR/In-Int)
  1146               Flag: 0x01 (Global label)
  2.2.2.9/32         Flag: 0x20 (No FRR/Node-ID)
  57.20.20.2/32      Flag: 0x00 (No FRR)
  57.20.20.1/32      Flag: 0x40 (No FRR/In-Int)
  3                  Flag: 0x01 (Global label)
  3.3.3.9/32         Flag: 0x20 (No FRR/Node-ID)
Fast Reroute protection: Ready
  FRR inner label: 3           Bypass tunnel: Tunnel253

Tunnel name: Sysname_t253
Destination: 3.3.3.9                    Source: 2.2.2.9
Tunnel ID: 253                          LSP ID: 17767
LSR type: Ingress                       Direction: Bidirectional, Downstream
Setup priority: 7                       Holding priority: 7
In-Label: -                             Out-Label: 1025
In-Interface: -                         Out-Interface: Vlan30
Nexthop: 10.11.112.135                  Exclude-any: 0
Include-Any: 0                          Include-all: 0
Mean rate (CIR): 125.00 kbps            Mean burst size (CBS): 0.00 bytes
```

```
Path MTU: 0                               Class type: CT0
RRO number: 8
  10.11.112.140/32   Flag: 0x00 (No FRR)
  10.11.112.135/32   Flag: 0x40 (No FRR/In-Int)
  1025               Flag: 0x01 (Global label)
  5.5.5.9/32         Flag: 0x20 (No FRR/Node-ID)
  57.40.40.3/32      Flag: 0x00 (No FRR)
  57.40.40.1/32      Flag: 0x40 (No FRR/In-Int)
  3                  Flag: 0x01 (Global label)
  3.3.3.9/32         Flag: 0x20 ((No FRR/Node-ID)
Fast Reroute protection: None
```

Table 7 Command output

Field	Description
Tunnel name	Tunnel name. The tunnel ingress node generates the name and notifies other nodes of the name through a Path message. When the ingress node is an H3C device, the tunnel name is *Sysname*_t*tunnel-ID*, where *Sysname* represents the device name, and *tunnel-ID* represents the ID of the tunnel. You can configure the device name by executing the **sysname** command in system view.
Destination	Tunnel destination address.
Source	Tunnel source address.
Direction	Tunnel direction: • **Unidirectional**—Unidirectional tunnel. • **Bidirectional, Downstream**—Forward CRLSP of a bidirectional tunnel. • **Bidirectional, Upstream**—Backward CRLSP of a bidirectional tunnel.
Exclude-any	Affinity representing a set of attribute filters. Matching any filter renders a link unacceptable.
Include-any	Affinity representing a set of attribute filters. Matching any filter renders a link acceptable.
Include-all	Affinity representing a set of attribute filters. All filters must be present for a link to be acceptable.
Class type	CT of the LSP.
RRO number	Number of Record Route Objects (RROs). If the number is not 0, the subsequent output displays the IP addresses or labels recorded in the RROs. The RRO information is displayed only when route recording is configured on the tunnel interface.
Flag	Flag value and its meaning in an RRO: • **No FRR**—FRR is not configured. • **FRR Avail**—FRR is available. • **In use**—FRR has occurred. • **BW**—Bandwidth protection. • **Node-Prot**—Node protection. • **Node-ID**—The IP address in the RRO is the LSR ID of the node. • **In-Int**—The IP address in the RRO is address of the incoming interface. • **Global label**—Per-platform label space.

Field	Description
Fast Reroute protection	Whether the tunnel has been bound to an FRR bypass tunnel: • **None**—Not bound to a bypass tunnel. • **Ready**—Bound to a bypass tunnel. No FRR has occurred. • **Active**—Bound to a bypass tunnel. An FRR has occurred.
FRR inner label	Incoming label of the FRR bypass tunnel. This field is displayed only when a bypass tunnel is bound.
Bypass tunnel	Name of the bypass tunnel. This field is displayed only when a bypass tunnel is bound.

Related commands

display rsvp request

display rsvp reservation

display rsvp sender

display rsvp peer

Use **display rsvp peer** to display RSVP neighbor information.

Syntax

display rsvp peer [**interface** *interface-type interface-number*] [**ip** *ip-address*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

interface *interface-type interface-number*: Displays information about RSVP neighbors connected to the interface specified by its type and number.

ip *ip-address*: Displays information about the RSVP neighbor specified by its IP address.

verbose: Displays detailed information about RSVP neighbors. If you do not specify this keyword, the command displays brief information about RSVP neighbors.

Usage guidelines

If you do not specify any parameters, this command displays brief information about all RSVP neighbors.

Examples

Display brief information about all RSVP neighbors.

```
<Sysname> display rsvp peer
Peer            Interface               State    Type     Summary refresh
57.10.10.1      Vlan10                  Idle     Active   Enabled
57.20.20.1      Vlan20                  Init     Passive  Disabled
```

Table 8 Command output

Field	Description
Peer	Address of the RSVP neighbor.
Interface	Interface connected to the RSVP neighbor.
State	Local hello state: • **Idle**—Hello extension is disabled. • **Init**—Hello extension is enabled. The local device failed to exchange hellos with the neighbor or hello exchanges are in progress. • **Up**—Hello extension is enabled. The local device successfully exchanged hellos with the neighbor.
Type	Role of the local device in the neighbor relationship: • **Active**—The local device actively sends hello requests to the neighbor. • **Passive**—The local end passively receives hello requests from the neighbor and replies with hello ACK messages.
Summary refresh	State of the Srefresh feature on the neighbor: **Enabled** or **Disabled**.

Display detailed information about all RSVP neighbors.

```
<Sysname> display rsvp peer verbose
Peer: 57.10.10.1                        Interface: Vlan10
Hello state: Idle                       Hello type: Active
P2P PSB count: 0                        P2P RSB count: 3
P2MP PSB count: 0                       P2MP RSB count: 0
Src instance: 0x32e                     Dst instance: 0x0
Summary refresh: Enabled                Graceful Restart state: Invalid
Peer GR restart time: 0 ms              Peer GR recovery time: 0 ms

Peer: 57.20.20.1                        Interface: Vlan20
Hello state: Init                       Hello type: Active
P2P PSB count: 0                        P2P RSB count: 1
P2MP PSB count: 0                       P2MP RSB count: 0
Src instance: 0x32e                     Dst instance: 0x0
Summary refresh: Disabled               Graceful Restart state: Ready
Peer GR restart time: 0 ms              Peer GR recovery time: 0 ms
```

Table 9 Command output

Field	Description
Peer	Address of the RSVP neighbor.
Interface	Interface connected to the RSVP neighbor.
Hello state	Local hello state: • **Idle**—Hello extension is disabled locally. • **Init**—Hello extension is enabled locally. The local device failed to exchange hellos with the neighbor or hello exchanges are in progress. • **Up**—Hello extension is enabled locally. The local device successfully exchanged hellos with the neighbor.

Field	Description
Hello type	Role of the local device in the neighbor relationship: • **Active**—The local device actively sends hello requests to the neighbor. • **Passive**—The local device passively receives hello requests from the neighbor and replies with hello ACK messages.
P2P PSB count	Number of PSBs for the P2P neighbor.
P2P RSB count	Number of RSBs for P2P the neighbor.
P2MP PSB count	This field is not supported in the current software version. Number of PSBs for the P2MP neighbor.
P2MP RSB count	This field is not supported in the current software version. Number of RSBs for the P2MP neighbor.
Src instance	Local device instance carried in the hello sent to the neighbor.
Dst instance	Neighbor device instance carried in the last hello received from the neighbor.
Summary refresh	State of the Srefresh feature on the neighbor: **Enabled** or **Disabled**.
Graceful Restart state	GR state of the neighbor: • **Invalid**—Neighbor is not GR capable, or GR is disabled locally. • **Ready**—Neighbor is GR capable. • **Restarting**—Neighbor is restarting. • **Recovering**—Neighbor is recovering.
Peer GR restart time	GR restart period of the neighbor, in milliseconds.
Peer GR recovery time	GR recovery period of the neighbor, in milliseconds.

display rsvp request

Use **display rsvp request** to display information about RSVP resource reservation requests sent to upstream devices.

Syntax

display rsvp request [**destination** *ip-address*] [**source** *ip-address*] [**tunnel-id** *tunnel-id*] [**prevhop** *ip-address*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

destination *ip-address*: Displays information about the RSVP resource reservation requests with the specified tunnel destination address.

source *ip-address*: Displays information about the RSVP resource reservation requests with the specified tunnel source address. The tunnel source address is the extended tunnel ID in the Session object of an RSVP message.

tunnel-id *tunnel-id*: Displays information about the RSVP resource reservation requests with the specified tunnel ID. The value range for a tunnel ID is 0 to 65535.

prevhop *ip-address*: Displays information about the RSVP resource reservation requests sent to the specified upstream device. The *ip-address* argument is the address of the destination device of the RSVP resource reservation requests, which is the address of the previous hop on the tunnel.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief information.

Usage guidelines

If you do not specify any parameters, this command displays brief information about all RSVP resource reservation requests sent to upstream devices.

Examples

Display brief information about the RSVP resource reservation requests sent to all upstream devices.

```
<Sysname> display rsvp request
Destination     Source          Tunnel-ID Previous-hop      Style
3.3.3.9         1.1.1.9         1         57.10.10.1        SE
```

Table 10 Command output

Field	Description
Destination	Tunnel destination address.
Source	Tunnel source address.
Style	Resource reservation style: • **SE**—Shared-explicit style. • **FF**—Fixed-filter style.

Display detailed information about the RSVP resource reservation requests sent to all upstream devices.

```
<Sysname> display rsvp request verbose
Destination: 3.3.3.9                    Source: 1.1.1.9
Tunnel ID: 1                            Style: SE
Previous hop: 57.10.10.1                Previous hop LIH: 0xf0008
Sent message epoch: 0                   Sent message ID: 0
Out-Interface: Vlan10                   Refresh interval: 30000 ms
Unknown object number: 0
Flow descriptor 1:
  Flow specification:
    Mean rate (CIR): 50.00 kbps         Mean burst size (CBS): 1000.00 bytes
    Path MTU: 1500                      QoS service: Controlled-Load
  Filter specification 1:
    Sender address: 1.1.1.9             LSP ID: 23
    Label: 1110
```

Table 11 Command output

Field	Description
Destination	Tunnel destination address.
Source	Tunnel source address.

Field	Description
Style	Resource reservation style: • **SE**—Shared-explicit style. • **FF**—Fixed-filter style.
Previous hop LIH	Logical interface handle of the previous hop.
Sent message epoch	Value of the Epoch field in the Message ID object of the sent message.
Sent message ID	Message ID in the sent message.
Out-Interface	Outgoing interface of the message.
Refresh interval	Refresh interval for Path and Resv messages, in milliseconds.
Unknown object number	Number of unknown objects.
QoS service	QoS service type: **Controlled-Load** or **Guaranteed**.
Sender address	Sender address identifies the tunnel source end.
Label	Incoming label of the LSP.

Related commands

display rsvp lsp

display rsvp reservation

display rsvp sender

display rsvp reservation

Use **display rsvp reservation** to display information about RSVP resource reservation states.

Syntax

display rsvp reservation [**destination** *ip-address*] [**source** *ip-address*] [**tunnel-id** *tunnel-id*] [**nexthop** *ip-address*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

destination *ip-address*: Displays information about the RSVP resource reservation states with the specified tunnel destination address.

source *ip-address*: Displays information about the RSVP resource reservation states with the specified tunnel source address. The tunnel source address is the extended tunnel ID in the Session object of an RSVP message.

tunnel-id *tunnel-id*: Displays information about the RSVP resource reservation states with the specified tunnel ID. The value range for a tunnel ID is 0 to 65535.

nexthop *ip-address*: Displays information about the RSVP resource reservation states received from the specified downstream device. The *ip-address* argument is the address of the device that sent the RSVP resource reservation states, which is the address of the next hop on the tunnel.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief information.

Usage guidelines

If you do not specify any parameters, this command displays brief information about all RSVP resource reservation states.

Examples

Display brief information about all RSVP resource reservation states.

```
<Sysname> display rsvp reservation
Destination     Source          Tunnel-ID Nexthop          Style
3.3.3.9         1.1.1.9         1         57.20.20.1       SE
```

Table 12 Command output

Field	Description
Destination	Tunnel destination address.
Source	Tunnel source address.
Style	Resource reservation style: • **SE**—Shared-explicit style. • **FF**—Fixed-filter style.

Display detailed information about all RSVP resource reservation states.

```
<Sysname> display rsvp reservation verbose
Destination: 3.3.3.9                    Source: 1.1.1.9
Tunnel ID: 1                            Style: SE
Nexthop: 57.20.20.1                     Nexthop LIH: 0x35
Received message epoch: 0               Received message ID: 0
In-Interface: Vlan10                    Unknown object number: 0
Flow descriptor 1:
  Flow specification:
    Mean rate (CIR): 50.00 kbps         Mean burst size (CBS): 1000.00 bytes
    Path MTU: 1500                      QoS service: Controlled-Load
  Filter specification 1:
    Sender address: 1.1.1.9             LSP ID: 23
    Label: 3
    RRO number: 3
      57.20.20.1/32      Flag: 0x40 (No FRR/In-Int)
      3                  Flag: 0x01 (Global label)
      3.3.3.9/32         Flag: 0x20 (No FRR/Node-ID)
```

Table 13 Command output

Field	Description
Destination	Tunnel destination address.
Source	Tunnel source address.

Field	Description
Style	Resource reservation style: • **SE**—Shared-explicit style. • **FF**—Fixed-filter style.
Nexthop LIH	Logical interface handle of the local outgoing interface for the next hop.
Received message epoch	Value of the Epoch field in the Message ID object of the received message.
Received message ID	Message ID in the received message.
In-Interface	Incoming interface of the message.
Unknown object number	Number of unknown objects.
QoS service	QoS service type: **Controlled-Load** or **Guaranteed**.
Sender address	Sender address identifies the tunnel source end.
Label	Outgoing label of the LSP.
RRO number	Number of RROs. If the number is not 0, the subsequent output displays the IP addresses or labels recorded in the RROs. The RRO information is displayed only when route recording is configured on the tunnel interface.
Flag	Flag value and its meaning in an RRO: • **No FRR**—FRR is not configured. • **FRR Avail**—FRR is available. • **In use**—FRR has occurred. • **BW**—Bandwidth protection. • **Node-Prot**—Node protection. • **Node-ID**—The IP address in the RRO is the LSR ID of the node. • **In-Int**—The IP address in the RRO is that of the incoming interface. • **Global label**—Per-platform label space.

Related commands

display rsvp lsp

display rsvp request

display rsvp sender

display rsvp sender

Use **display rsvp sender** to display information about RSVP path states.

Syntax

display rsvp sender [**destination** *ip-address*] [**source** *ip-address*] [**tunnel-id** *tunnel-id*] [**lsp-id** *lsp-id*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

destination *ip-address*: Displays information about the RSVP path states with the specified tunnel destination address.

source *ip-address*: Displays information about the RSVP path states with the specified tunnel source address. The tunnel source address is the extended tunnel ID in the Session object of an RSVP message.

tunnel-id *tunnel-id*: Displays information about the RSVP path states with the specified tunnel ID. The value range for a tunnel ID is 0 to 65535.

lsp-id *lsp-id*: Displays information about the RSVP path states with the specified LSP ID. The *lsp-id* argument specifies the ID of a CRLSP, in the range of 0 to 65535.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief information.

Usage guidelines

If you do not specify any parameters, this command displays brief information about all RSVP path states.

Examples

Display brief information about all RSVP path states.

```
<Sysname> display rsvp sender
Destination     Source          Tunnel-ID LSP-ID  Style     Bitrate
3.3.3.9         1.1.1.9         1         5       SE        0.00
3.3.3.9         2.2.2.9         253       17767   SE        125.00
```

Table 14 Command output

Field	Description
Destination	Tunnel destination address.
Source	Tunnel source address.
Style	Resource reservation style: • **SE**—Shared-explicit style. • **FF**—Fixed-filter style.
Bitrate	Tunnel bandwidth in kbps.

Display detailed information about all RSVP path states.

```
<Sysname> display rsvp sender verbose
Destination: 3.3.3.9                    Source: 1.1.1.9
Tunnel ID: 1                            Style: SE
Sender address: 1.1.1.9                 LSP ID: 5
Setup priority: 7                       Holding priority: 7
FRR desired: Yes                        BW protection desired: Yes
Received upstream label: 1051           Sent upstream label: 1051
Previous hop: 57.10.10.1                Previous hop LIH: 0xf0008
Mean rate (CIR): 0.00 kbps              Mean burst size (CBS): 1000.00 bytes
MTU: 1500                               Qos service: Controlled-Load
Received message epoch: 0               Received message ID: 0
Sent message epoch: 0                   Sent message ID: 0
```

```
In-Interface: Vlan10                    Local LIH: 0x35
Local address: 57.20.20.2               Refresh interval: 30000 ms
Out-Interface: Vlan20                   Nexthop: 57.20.20.1
Unknown object number: 0
Received ERO number: 2
  57.10.10.2/32      Strict
  57.20.20.1/32      Loose
Sent ERO number: 1
  57.20.20.1/32      Loose
XRO number: 2
  67.10.10.1/32
  67.20.20.1/32
RRO number: 1
  57.10.10.1/32      Flag: 0x00 (No FRR)
Fast Reroute PLR: Active
  FRR inner label: 3                    Bypass tunnel: Tunnel253
  Sender Template:
    Sender address: 10.11.112.140       LSP ID: 5
  FRR ERO number: 1
    3.3.3.9/32         Strict
Fast Reroute MP: None

Destination: 3.3.3.9                    Source: 2.2.2.9
Tunnel ID: 253                          Style: SE
Sender address: 2.2.2.9                 LSP ID: 17767
Setup priority: 7                       Holding priority: 7
FRR desired: Yes                        BW protection desired: Yes
Received upstream label: 1115           Sent upstream label: 1115
Previous hop: 57.10.10.1                Previous hop LIH: 0xf0008
Mean rate (CIR): 125.00 kbps            Mean burst size (CBS): 0.00 bytes
MTU: 1500                               Qos service: Controlled-Load
Received message epoch: 0               Received message ID: 0
Sent message epoch: 0                   Sent message ID: 0
In-Interface: Vlan10                    Local LIH: 0x67
Local address: 10.11.112.140            Refresh interval: 30000 ms
Out-Interface: Vlan30                   Nexthop: 10.11.112.135
Unknown object number: 0
Received ERO number: 5
  2.2.2.9/32         Strict
  10.11.112.140/32   Strict
  10.11.112.135/32   Strict
  57.40.40.3/32      Strict
  57.40.40.1/32      Strict
Sent ERO number: 3
  10.11.112.135/32   Strict
  57.40.40.3/32      Strict
  57.40.40.1/32      Strict
XRO number: 1
```

```
  67.40.40.1/32
RRO number: 0
Fast Reroute PLR: None
Fast Reroute MP: Active
  In-Interface: Vlan10
  Sender Template:
    Sender address: 10.11.112.140         LSP ID: 5
```

Table 15 Command output

Field	Description
Destination	Tunnel destination address.
Source	LSR ID of the device at the tunnel source end.
Style	Resource reservation style: • **SE**—Shared-explicit style. • **FF**—Fixed-filter style.
Sender address	Sender address identifies the tunnel source end.
FRR desired	State of FRR: **Yes** or **No**.
BW protection desired	State of bandwidth protection: **Yes** or **No**.
Received upstream label	Backward LSP label received from the upstream device.
Sent upstream label	Backward LSP label sent to the downstream device.
Previous hop LIH	Logical interface handle of the previous hop.
QoS service	QoS service type: **Controlled-Load** or **Guaranteed**.
Received message Epoch	Value of the Epoch field in the Message ID object of the received message.
Received message ID	Message ID in the received message.
Sent message epoch	Value of the Epoch field in the Message ID object of the sent message.
Sent message ID	Message ID in the sent message.
In-Interface	Incoming interface of the message.
Local LIH	Local logical interface handle.
Local address	IP address of the outgoing interface of the Path message.
Refresh interval	Refresh interval for Path and Resv messages, in milliseconds.
Out-Interface	Outgoing interface of the message.
Unknown object number	Number of unknown objects.
Received ERO number	Number of received Explicit Route Objects (EROs) and the ERO information. ERO information includes the addresses of the nodes on the explicit path, and whether the current node is a loose or strict next hop.
Sent ERO number	Number of sent EROs and the ERO information. ERO information includes the addresses of the nodes on the explicit path, and whether the current node is a loose or strict next hop.

Field	Description
XRO number	Number of Exclude Route Objects (XROs). If the number is not 0, the subsequent output displays the IP addresses in the XROs. The IP addresses are the addresses of interfaces or the LSR IDs of the nodes that are to be excluded from routes. The addresses in the XROs are non-sequenced.
RRO number	Number of Record Route Objects (RROs). If the number is not 0, the subsequent output displays the IP addresses or labels recorded in the RROs. The RRO information is displayed only when route recording is configured on the tunnel interface.
Flag	Flag value and its meaning in an RRO: • **No FRR**—FRR is not configured. • **FRR Avail**—FRR is available. • **In use**—FRR has occurred. • **BW**—Bandwidth protection. • **Node-Prot**—Node protection. • **Node-ID**—The IP address in the RRO is the LSR ID of the node. • **In-Int**—The IP address in the RRO is that of the incoming interface. • **Global label**—Per-platform label space.
Fast Reroute PLR	Point of Local Repair (PLR) information: • **None**—Not bound to an FRR bypass tunnel. • **Ready**—Bound to an FRR bypass tunnel. No FRR has occurred. • **Active**—Bound to an FRR bypass tunnel. An FRR has occurred.
FRR inner label	Incoming label of the FRR bypass tunnel. Only the PLR node displays this field.
Bypass tunnel	Name of the bypass tunnel. Only the PLR node displays this field.
Sender address	Address of the Path message sender after an FRR. The value of this field is the address of the outgoing interface of the bypass tunnel on the PLR node.
LSP ID	LSP ID carried in the Path message after an FRR.
Fast Reroute MP	Merge Point (MP) information: • **Active**—The node is an MP and an FRR has occurred. • **None**—The node is not an MP, or the node is an MP but no FRR has occurred.
In-Interface	Incoming interface of the message.

Related commands

`display rsvp lsp`

`display rsvp request`

`display rsvp reservation`

display rsvp statistics

Use **`display rsvp statistics`** to display RSVP statistics.

Syntax

display rsvp statistics [**interface** [*interface-type interface-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

mdc-admin

mdc-operator

Parameters

interface: Displays RSVP statistics on interfaces. If you do not specify this keyword, the command displays global RSVP statistics.

interface-type interface-number: Displays RSVP statistics on the interface specified by its type and number. If you specify the **interface** keyword without this argument, the command displays RSVP statistics on all RSVP-enabled interfaces.

Examples

Display global RSVP statistics.

```
<Sysname> display rsvp statistics
P2P statistics:
Object                Added           Deleted
  PSB                 3               1
  RSB                 3               1
  LSP                 3               1
P2MP statistics:
Object                Added           Deleted
  PSB                 0               0
  RSB                 0               0
  LSP                 0               0

Packet                Received        Sent
  Path                5               5
  Resv                5               5
  PathError           0               0
  ResvError           0               0
  PathTear            0               0
  ResvTear            0               0
  ResvConf            0               0
  Bundle              0               0
  Ack                 0               0
  Srefresh            0               0
  Hello               0               0
  Challenge           0               0
  Response            0               0
  Error               0               0
```

Display RSVP statistics on interfaces.

```
<Sysname> display rsvp statistics interface
Vlan10:
Packet                  Received         Sent
  Path                  2                2
  Resv                  2                2
  PathError             0                0
  ResvError             0                0
  PathTear              0                0
  ResvTear              0                0
  ResvConf              0                0
  Bundle                0                0
  Ack                   0                0
  Srefresh              0                0
  Hello                 0                0
  Challenge             0                0
  Response              0                0
  Error                 0                0

Vlan20:
Packet                  Received         Sent
  Path                  3                3
  Resv                  3                3
  PathError             0                0
  ResvError             0                0
  PathTear              0                0
  ResvTear              0                0
  ResvConf              0                0
  Bundle                0                0
  Ack                   0                0
  Srefresh              0                0
  Hello                 0                0
  Challenge             0                0
  Response              0                0
  Error                 0                0
```

Table 16 Command output

Field	Description
P2P statistics	P2P statistics.
PSB	Number of added/deleted PSBs.
RSB	Number of added/deleted RSBs.
LSP	Number of added/deleted LSPs.
P2MP statistics	This field is not supported in the current software version. P2MP statistics.
Path	Number of received/sent Path messages.
Resv	Number of received/sent Resv messages.
PathError	Number of received/sent Path Error messages.

Field	Description
ResvError	Number of received/sent Resv Error messages.
PathTear	Number of received/sent Path Tear messages.
ResvTear	Number of received/sent Resv Tear messages.
ResvConf	Number of received/sent Resv Conf messages.
Bundle	Number of received/sent Bundle messages.
Ack	Number of received/sent Ack messages.
Srefresh	Number of received/sent Srefresh messages.
Hello	Number of received/sent Hello messages.
Challenge	Number of received/sent Integrity Challenge messages.
Response	Number of received/sent Integrity Response messages.
Error	Number of received/sent error messages.

Related commands

reset rsvp statistics

dscp

Use **dscp** to set a DSCP value for outgoing RSVP packets.

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

Syntax

dscp *dscp-value*

undo dscp

Default

The DSCP value for outgoing RSVP packets is 48.

Views

RSVP view

Predefined user roles

network-admin

mdc-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Usage guidelines

The DSCP value of an IP packet specifies the priority level of the packet and affects the transmission priority of the packet.

Examples

Set the DSCP value for outgoing RSVP packets to 56.

```
<Sysname> system-view
[Sysname] rsvp
[Sysname-rsvp] dscp 56
```

Related commands

display rsvp

graceful-restart enable

Use **graceful-restart enable** to enable RSVP GR.

Use **undo graceful-restart enable** to disable RSVP GR.

Syntax

graceful-restart enable

undo graceful-restart enable

Default

RSVP GR is disabled.

Views

RSVP view

Predefined user roles

network-admin

mdc-admin

Usage guidelines

RSVP supports only the GR helper feature. The device is not able to perform GR, but it can help neighbor devices to perform GR.

Nonstop forwarding (NSF) is implemented between active and standby processes on the device.

The local device can act as a GR helper for the RSVP neighbor connected to an interface only after the following features are enabled on that interface:

- RSVP GR (configured by the **graceful-restart enable** command).
- RSVP hello extension (configured by the **rsvp hello enable** command).

Examples

Enable RSVP GR globally.

```
<Sysname> system-view
[Sysname] rsvp
[Sysname-rsvp] graceful-restart enable
```

Related commands

rsvp hello enable

hello interval

Use **hello interval** to set the interval for sending hello requests.

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

Syntax

hello interval *interval*

undo hello interval

Default

Hello request messages are sent at an interval of 5 seconds.

Views

RSVP view

Predefined user roles

network-admin

mdc-admin

Parameters

interval: Specifies the interval at which RSVP sends hello requests, in the range of 1 to 60 seconds.

Usage guidelines

If no hello request is received from a neighbor within the hello interval, the device sends a hello request to the neighbor. If the device receives a hello request from a neighbor within the interval, it immediately replies the neighbor with a hello ACK message.

The **hello interval** command takes effect only on interfaces that have the RSVP hello extension feature enabled (by using the **rsvp hello enable** command).

Examples

Set the interval for sending hello request messages to 10 seconds.

```
<Sysname> system-view
[Sysname] rsvp
[Sysname-rsvp] hello interval 10
```

Related commands

hello lost

rsvp hello enable

hello lost

Use **hello lost** to set the maximum number of consecutive lost or erroneous hellos.

Use **undo hello lost** to restore the default.

Syntax

hello lost *times*

undo hello lost

Default

The maximum number of consecutive lost or erroneous hellos is 4.

Views

RSVP view

Predefined user roles

network-admin

mdc-admin

Parameters

times: Specifies the maximum number of consecutive lost or erroneous hellos, in the range of 3 to 10.

Usage guidelines

When a device sends a hello to a neighbor but the device does not receive any replies within an interval, the hello is lost. The device determines that the neighbor fails when the number of consecutive lost hellos or erroneous hellos from the neighbor reaches the maximum (configured by this command).

If RSVP GR is enabled, the local device acts as a GR helper to help the neighbor to perform GR. If RSVP GR is disabled but FRR is enabled on the local device, it performs an FRR.

This command takes effect only after the RSVP hello extension feature has been enabled by using the **rsvp hello enable** command.

If the maximum number is too big, neighbor failures cannot be promptly detected. If the maximum number is too small, an operating neighbor might be regarded failed.

Examples

Set the maximum number of consecutive lost or erroneous hellos to 6.

```
<Sysname> system-view
[Sysname] rsvp
[Sysname-rsvp] hello lost 6
```

Related commands

hello interval

rsvp hello enable

keep-multiplier

Use **keep-multiplier** to set the PSB and RSB timeout multiplier.

Use **undo keep-multiplier** to restore the default.

Syntax

keep-multiplier *number*

undo keep-multiplier

Default

The PSB and RSB timeout multiplier is 3.

Views

RSVP view

Predefined user roles

network-admin

mdc-admin

Parameters

number: Specifies the PSB and RSB timeout multiplier in the range of 3 to 255.

Usage guidelines

The PSB and RSB timeout is computed in this formula: Timeout = (keep-multiplier+0.5) × 1.5 × refresh-time. Refresh-time is the interval at which the peer device advertises the Path and Resv messages to the local device.

To prevent too many PSBs and RSBs from occupying system resources, the device removes a PSB or RSB if no Path or Resv message is received within the timeout interval.

Examples

Set the PSB and RSB timeout multiplier to 5.

```
<Sysname> system-view
[Sysname] rsvp
[Sysname-rsvp] keep-multiplier 5
```

Related commands

refresh interval

peer

Use **peer** to create an RSVP authentication neighbor and enter its view, or enter the view of an existing RSVP authentication neighbor.

Use **undo peer** to delete an RSVP authentication neighbor.

Syntax

peer *ip-address*

undo peer *ip-address*

Default

No RSVP authentication neighbors exist.

Views

RSVP view

Predefined user roles

network-admin

mdc-admin

Parameters

ip-address: Specifies an RSVP authentication neighbor by its IP address.

Usage guidelines

After this command is executed, you can configure RSVP authentication information for the specified RSVP neighbor, such as the authentication key and idle timeout of the security association.

After the device receives an RSVP message with an authentication object, it checks whether it has an RSVP authentication neighbor that matches one of the following addresses:

- The IP address in PHOP of the message (Path or Path Tear message).
- The source IP address in the message (message other than Path and Path Tear).

If a matching neighbor exists and an authentication key has been configured for the neighbor, the device verifies the validity of the message according to the key. If no authentication key is configured for the neighbor, the device uses the authentication key configured in interface view or RSVP view to verify the message validity. If no authentication key is configured in any view, the device ignores the authentication object carried in the message and accepts the message.

When sending an RSVP message, the device checks whether it has a matching authentication neighbor according to the next hop address for the destination address in the RSVP message. If a matching neighbor exists and an authentication key has been configured for the neighbor, the device sets the authentication object of the message according to the key. If no authentication key is configured for the neighbor, the device uses the authentication key configured in interface view or

RSVP view to set the authentication object. If no authentication key is configured in any view, the device does not add an authentication object in the message.

If an FRR occurs, the downstream authentication neighbor of the PLR node is the destination IP address of the bypass tunnel. The upstream authentication neighbor of the MP node is the IP address of the physical outgoing interface of the bypass tunnel on the PLR.

Examples

Create RSVP authentication neighbor 1.1.1.1, enter RSVP neighbor view, and configure a plaintext authentication key of **abcdfegh** for the neighbor.

```
<Sysname> system-view
[Sysname] rsvp
[Sysname-rsvp] peer 1.1.1.1
[Sysname-rsvp-peer-1.1.1.1] authentication key plain abcdfegh
```

Related commands

authentication challenge

authentication key

authentication lifetime

authentication window-size

refresh interval

Use **refresh interval** to set the refresh interval for Path and Resv messages.

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

Syntax

refresh interval *interval*

undo refresh interval

Default

The refresh interval for Path and Resv messages is 30 seconds.

Views

RSVP view

Predefined user roles

network-admin

mdc-admin

Parameters

interval: Specifies the interval at which RSVP refreshes Path and Resv messages, in the range of 10 to 65535 seconds.

Usage guidelines

This command performs the following operations:

- Determines the interval for sending Path and Resv messages.
- Adds the locally configured refresh interval in the sent Path and Resv messages, so the peer device can use this value to calculate the PSB and RSB timeout.

Examples

Set the refresh interval for Path and Resv messages to 60 seconds.

```
<Sysname> system-view
[Sysname] rsvp
[Sysname-rsvp] refresh interval 60
```

Related commands

keep-multiplier

reset rsvp authentication

Use **reset rsvp authentication** to clear RSVP security associations.

Syntax

reset rsvp authentication [**from** *ip-address* **to** *ip-address*]

Views

User view

Predefined user roles

network-admin

mdc-admin

Parameters

from *ip-address*: Clears the RSVP security associations with the specified authentication source IP address.

to *ip-address*: Clears the RSVP security associations with the specified authentication destination IP address.

Usage guidelines

If you do not specify the **from** *ip-address* **to** *ip-address* options, this command clears the security associations established with all RSVP neighbors.

Examples

Clear all RSVP security associations.

```
<Sysname> reset rsvp authentication
```

Clear the RSVP security association sourced from 1.1.1.1 to 2.2.2.2.

```
<Sysname> reset rsvp authentication from 1.1.1.1 to 2.2.2.2
```

Related commands

display rsvp authentication

reset rsvp statistics

Use **reset rsvp statistics** to clear RSVP statistics.

Syntax

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

Views

User view

Predefined user roles

network-admin

mdc-admin

Parameters

interface: Clears RSVP statistics on interfaces. If you do not specify this keyword, the command clears global RSVP statistics.

interface-type interface-number: Clears RSVP statistics on the interface specified by its type and number. If you specify the **interface** keyword without this argument, the command clears RSVP statistics on all RSVP-enabled interfaces.

Examples

Clear global RSVP statistics.

```
<Sysname> reset rsvp statistics
```

Clear RSVP statistics on all RSVP-enabled interfaces.

```
<Sysname> reset rsvp statistics interface
```

Related commands

display rsvp statistics

rsvp

Use **rsvp** to enable RSVP globally and enter RSVP view.

Use **undo rsvp** to disable RSVP globally.

Syntax

rsvp

undo rsvp

Default

RSVP is disabled globally.

Views

System view

Predefined user roles

network-admin

mdc-admin

Usage guidelines

To enable global RSVP, you must enable both global RSVP (by using the **rsvp** command) and global MPLS TE (by using the **mpls te** command).

Examples

Enable RSVP globally and enter RSVP view.

```
<Sysname> system-view
[Sysname] rsvp
[Sysname-rsvp]
```

Related commands

mpls te

rsvp enable

rsvp authentication challenge

Use **rsvp authentication challenge** to enable RSVP challenge-response handshake on an interface.

Use **undo rsvp authentication challenge** to disable RSVP challenge-response handshake on an interface.

Syntax

rsvp authentication challenge

undo rsvp authentication challenge

Default

RSVP challenge-response handshake is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Usage guidelines

To prevent packet replay attacks, RSVP requires received authentication messages to carry incremental sequence numbers. RSVP saves the sequence number of the last valid message in a receive-type security association to verify the subsequent messages. However, when RSVP creates a new receive-type security association, it cannot obtain the sequence number of the sender. To successfully establish the receive-type security association, RSVP sets the receive sequence number to 0 by default. Then, the association can receive a message with any sequence number from the peer. Because this introduces a vulnerability to replay attacks, you should execute the **authentication challenge** command. When RSVP creates a receive-type security association, it will perform a challenge-response handshake to obtain the sequence number of the sender.

RSVP challenge-response handshake can be configured in the following views:

- **RSVP view**—Configuration applies to all RSVP security associations.
- **RSVP neighbor view**—Configuration applies only to RSVP security associations with the specified RSVP neighbor.
- **Interface view**—Configuration applies only to RSVP security associations established on the current interface.

Examples

Enable RSVP challenge-response handshake on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rsvp authentication challenge
```

Related commands

authentication challenge

authentication key

authentication lifetime

authentication window-size

display rsvp authentication

reset rsvp authentication

rsvp authentication key

rsvp authentication lifetime

rsvp authentication window-size

rsvp authentication key

Use **rsvp authentication key** to enable RSVP authentication on an interface and configure the authentication key.

Use **undo rsvp authentication key** to disable RSVP authentication on an interface.

Syntax

rsvp authentication key { **cipher** | **plain** } *string*

undo rsvp authentication key

Default

RSVP authentication is disabled.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Parameters

cipher: Specifies an authentication key in encrypted form.

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

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

Usage guidelines

RSVP authentication ensures integrity of RSVP messages, preventing fake resource reservation requests from occupying network resources.

RSVP uses MD5 to calculate a digest for the authentication key and the message body, adds the digest to the message, and sends the message. When the peer receives the message, it performs the same calculation and compares the calculated digest with the digest in the message. If the two digests are the same, the message passes the RSVP authentication and is accepted. If the two digests are different, the peer device discards the message.

RSVP authentication can be configured in the following views:

- **RSVP view**—Configuration applies to all RSVP security associations.
- **RSVP neighbor view**—Configuration applies only to RSVP security associations with the specified RSVP neighbor.
- **Interface view**—Configuration applies only to RSVP security associations established on the current interface.

Configurations in RSVP neighbor view, interface view, and RSVP view are in descending order of priority. If RSVP authentication for a neighbor is enabled in both RSVP neighbor view and RSVP view, the authentication key configured in RSVP neighbor view is used.

To re-establish a security association, you must delete the authentication key used by the current security association or delete the current security association (using the **reset rsvp authentication** command). Then, the device can re-establish a security association by looking up a new authentication key in order of priorities.

After RSVP authentication is enabled on the local device, you must also enable RSVP authentication and configure the same authentication key on the RSVP neighbor.

Examples

Enable RSVP authentication and configure an authentication key of **abcdefgh** on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rsvp authentication key plain abcdefgh
```

Related commands

authentication challenge

authentication key

authentication lifetime

authentication window-size

display rsvp authentication

reset rsvp authentication

rsvp authentication challenge

rsvp authentication lifetime

rsvp authentication window-size

rsvp authentication lifetime

Use **rsvp authentication lifetime** to set the idle timeout for RSVP security associations on an interface.

Use **undo rsvp authentication lifetime** to restore the default.

Syntax

rsvp authentication lifetime *life-time*

undo rsvp authentication lifetime

Default

The idle timeout for RSVP security associations is 1800 seconds on an interface.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Parameters

life-time: Specifies the RSVP security association idle timeout in the range of 30 to 86400 seconds.

Usage guidelines

When RSVP authentication is enabled, the device dynamically establishes security associations when receiving and sending RSVP messages to record the message sequence numbers, which are used in RSVP authentication.

To release memory resources, each security association has an idle timeout. When a security association is idle for the specified timeout time, the device deletes the security association. When the device sends or receives an authenticated RSVP message, it resets the idle timeout timer for the corresponding security association.

The RSVP authentication idle timeout can be configured in the following views:

- **RSVP view**—Configuration applies to all RSVP security associations.
- **RSVP neighbor view**—Configuration applies only to RSVP security associations with the specified RSVP neighbor.
- **Interface view**—Configuration applies only to RSVP security associations established on the current interface.

An RSVP security association established by using the authentication key configured in a view uses the idle timeout configured in the same view.

A modification to the idle timeout affects only security associations established after the modification. To apply the modification to existing security associations, you must execute the **reset rsvp authentication** command to delete and then re-establish the security associations.

Examples

Set the idle timeout for RSVP security associations to 100 seconds on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rsvp authentication lifetime 100
```

Related commands

authentication challenge

authentication key

authentication lifetime

authentication window-size

display rsvp authentication

reset rsvp authentication

rsvp authentication challenge

rsvp authentication key

rsvp authentication window-size

rsvp authentication window-size

Use **rsvp authentication window-size** to set the RSVP authentication window size, which is the maximum number of authenticated RSVP messages that can be received out of sequence on an interface.

Use **undo rsvp authentication window-size** to restore the default.

Syntax

rsvp authentication window-size *number*

undo rsvp authentication window-size

Default

Only one authenticated RSVP message can be received out of sequence on an interface.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Parameters

number: Specifies the maximum number of authenticated RSVP messages that can be received out of sequence, in the range of 1 to 64.

Usage guidelines

To protect against replay attacks, the sender places a unique sequence number in each RSVP message that contains authentication information. The sender increases the value of the sequence number by one each time it sends an RSVP message. If the sequence number of a received message is in the specified authentication window size, the receiver accepts the message. If it is not in the specified authentication window size, the receiver discards the message.

When the receiver receives an RSVP message, it compares the sequence number of the last accepted RSVP message with the sequence number of the newly received RSVP message.

- If the new sequence number is greater than the last sequence number, RSVP accepts the message and updates the last sequence number with the new sequence number.
- If the received sequence number equals the last sequence number, RSVP regards the message a replay message and discards the message.
- If the new sequence number is smaller than the last sequence number but greater than the new sequence number minus the window size, and has never been received before, RSVP accepts the message. If the new sequence number has been received before, RSVP regards the message a replay message and discards the message.
- If the new sequence number is smaller than the new sequence number minus the window size, RSVP regards the message invalid and discards the message.

By default, the authentication window size is 1. If the sequence number of a newly received RSVP message is smaller than that of the last accepted message, the device discards the message.

If the sender sends multiple RSVP messages in a short time, these messages might arrive at the neighbor out of sequence. If you use the default window size, the out-of-sequence messages will be discarded. To solve this problem, you can use the **rsvp authentication window-size** command to configure a correct window size.

A security association established by using the authentication key configured in a view uses the window size configured in that view.

A modification to the window size affects only security associations established after the modification. To apply the new setting to existing security associations, you must execute the **reset rsvp authentication** command to delete and then re-establish the security associations.

Examples

Set the maximum number of out-of-sequence authenticated RSVP messages that can be received on VLAN-interface 10 to 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rsvp authentication window-size 10
```

Related commands

authentication challenge

authentication key

authentication lifetime

authentication window-size

display rsvp authentication

reset rsvp authentication

rsvp authentication challenge

rsvp authentication key

rsvp authentication lifetime

rsvp bfd enable

Use **rsvp bfd enable** to enable BFD for RSVP on an interface.

Use **undo rsvp bfd enable** to restore the default.

Syntax

rsvp bfd enable

undo rsvp bfd enable

Default

RSVP-TE does not use BFD to detect the link status to an RSVP neighbor.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Usage guidelines

By sending hellos, RSVP cannot promptly detect neighbor status. By executing this command on an interface, a BFD session is established to detect the link status to the RSVP neighbor on the interface. When the neighbor fails, BFD can quickly detect the failure and notify RSVP of the failure so RSVP can respond as configured, for example, performs an FRR.

Examples

Enable BFD to detect the link status to the RSVP neighbor on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rsvp bfd enable
```

rsvp enable

Use **rsvp enable** to enable RSVP on an interface.

Use **undo rsvp enable** to disable RSVP on an interface.

Syntax

rsvp enable

undo rsvp enable

Default

RSVP is disabled on an interface.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Usage guidelines

Before you enable RSVP on an interface, you must first enable RSVP globally by using the **rsvp** command in system view.

Examples

Enable RSVP on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] rsvp
[Sysname-rsvp] quit
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rsvp enable
```

Related commands

rsvp

rsvp hello enable

Use **rsvp hello enable** to enable RSVP hello extension.

Use **undo rsvp hello enable** to disable RSVP hello extension.

Syntax

rsvp hello enable

undo rsvp hello enable

Default

RSVP hello extension is disabled.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Usage guidelines

With RSVP hello extension enabled, an interface sends and receives hello messages to detect the neighbor status.

Examples

Enable RSVP hello extension on VLAN-interface 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rsvp hello enable
```

Related commands

hello interval

hello lost

rsvp reduction retransmit increment

Use **rsvp reduction retransmit increment** to set the RSVP message retransmission increment value.

Use **undo rsvp reduction retransmit increment** to restore the default.

Syntax

rsvp reduction retransmit increment *increment-value*

undo rsvp reduction retransmit increment

Default

The RSVP message retransmission increment is 1.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Parameters

increment-value: Specifies the RSVP message retransmission increment in the range of 1 to 10.

Usage guidelines

After the **rsvp reduction srefresh reliability** command is executed, the retransmission increment and retransmission interval together determine the time for the next transmission of the RSVP message. For more information, see the usage guidelines in the rsvp reduction srefresh command.

Examples

On VLAN-interface 10, set the RSVP message retransmission increment value to 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rsvp reduction retransmit increment 2
```

Related commands

rsvp reduction retransmit interval

rsvp reduction srefresh

rsvp reduction retransmit interval

Use **rsvp reduction retransmit interval** to set the RSVP message retransmission interval.

Use **undo rsvp reduction retransmit interval** to restore the default.

Syntax

rsvp reduction retransmit interval *interval*

undo rsvp reduction retransmit interval

Default

The RSVP message retransmission interval is 500 milliseconds.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Parameters

interval: Specifies the RSVP message retransmission interval in the range of 500 to 3000 milliseconds.

Usage guidelines

After the **rsvp reduction srefresh reliability** command is executed, the retransmission increment and retransmission interval together determine the time for the next transmission of the RSVP message. For more information, see the usage guidelines in the rsvp reduction srefresh command.

Examples

On VLAN-interface 10, set the RSVP message retransmission interval to 1000 milliseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rsvp reduction retransmit interval 1000
```

Related commands

rsvp reduction retransmit increment

rsvp reduction srefresh

rsvp reduction srefresh

Use **rsvp reduction srefresh** to enable summary refresh and reliable RSVP message delivery.

Use **undo rsvp reduction srefresh** to disable summary refresh and reliable RSVP message delivery.

Syntax

rsvp reduction srefresh [**reliability**]

undo rsvp reduction srefresh

Default

Summary refresh and reliable RSVP message delivery are disabled.

Views

Interface view

Predefined user roles

network-admin

mdc-admin

Parameters

reliability: Enables reliable RSVP message delivery. If you do not specify this keyword, the command enables only the summary refresh feature.

Usage guidelines

RSVP sends Path and Resv messages with the same states and objects to maintain the path and reservation states at intervals (configured by the **refresh interval** command). These messages are collectively referred to as refresh messages. Refresh messages are used to synchronize the path and reservation states on RSVP neighbors and to recover from lost RSVP messages.

When multiple RSVP sessions exist on a network, the periodically sent refresh messages can cause network degradation. In this case, the refreshing interval of Path and Resv messages should not be too short. However, delay sensitive applications want to recover from lost RSVP messages through the refresh messages as soon as possible. In this case, the refreshing interval should not be too long. You can use the summary refresh (Srefresh) and the reliable RSVP message delivery features to find the appropriate balance.

Srefresh is implemented by adding a Message_ID object to a Path or Resv message to uniquely identify the message. To refresh Path and Resv states, RSVP does not need to send standard Path and Resv messages. Instead, it can send a summary refresh message at regular intervals (configured by the **refresh interval** command). The message carries a set of Message_ID objects that identify the Path and Resv states to be refreshed. The Srefresh feature reduces the number of refresh messages on the network and speeds up the refresh message processing.

Reliable RSVP message delivery requires the peer device to acknowledge each RSVP message received from the local device. If no acknowledgment is received, the local device retransmits the message.

To implement reliable RSVP message delivery, a node sends an RSVP message that includes a Message_ID object in which the ACK_Desired flag is set. The receiver needs to confirm the delivery by sending back a message that includes the Message_ID_ACK object. If the sender does not receive a Message_ID_ACK within the retransmission interval (Rf), it performs the following operations:

- Retransmits the message when Rf expire.
- Sets the next transmission interval to (1 + delta) × Rf.

The sender repeats this process until it receives the Message_ID_ACK before the retransmission time expires or it has transmitted the message three times.

The initial value of Rf is configured by the **rsvp reduction retransmit interval** command. The delta value is configured by the **rsvp reduction retransmit increment** command.

After the summary refresh is enabled, RSVP maintains the path and reservation states by sending Srefresh messages rather than standard refresh messages.

Examples

On VLAN-interface 10, enable summary refresh and reliable RSVP message delivery.

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

```
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rsvp reduction srefresh reliability
```

Related commands

refresh interval

rsvp reduction retransmit increment

rsvp reduction retransmit interval