



RSVP Message Authentication

The Resource Reservation Protocol (RSVP) Message Authentication feature provides a secure method to control quality of service (QoS) access to a network.

Feature Specifications for RSVP Message Authentication

Feature History

Release	Modification
12.2(15)T	This feature was introduced.

Supported Platforms

For platforms supported in Cisco IOS Release 12.2(15)T, consult Cisco Feature Navigator.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for RSVP Message Authentication, page 1](#)
- [Restrictions for RSVP Message Authentication, page 2](#)
- [Information About RSVP Message Authentication, page 2](#)
- [How to Configure RSVP Message Authentication, page 5](#)
- [Configuration Examples for RSVP Message Authentication, page 16](#)
- [Additional References, page 18](#)
- [Command Reference, page 20](#)
- [Glossary, page 40](#)

Prerequisites for RSVP Message Authentication

Ensure that RSVP is configured on two or more routers within the network before you can use the RSVP Message Authentication feature.

Restrictions for RSVP Message Authentication

- The RSVP Message Authentication feature is only for authenticating RSVP neighbors.
- The RSVP Message Authentication feature cannot discriminate between various QoS applications or users, of which many may exist on an authenticated RSVP neighbor.

Information About RSVP Message Authentication

To configure RSVP Message Authentication, you need to understand the following concepts:

- [Feature Design of RSVP Message Authentication, page 2](#)
- [Special Considerations for RSVP Message Authentication, page 4](#)
- [Benefits of RSVP Message Authentication, page 4](#)

Feature Design of RSVP Message Authentication

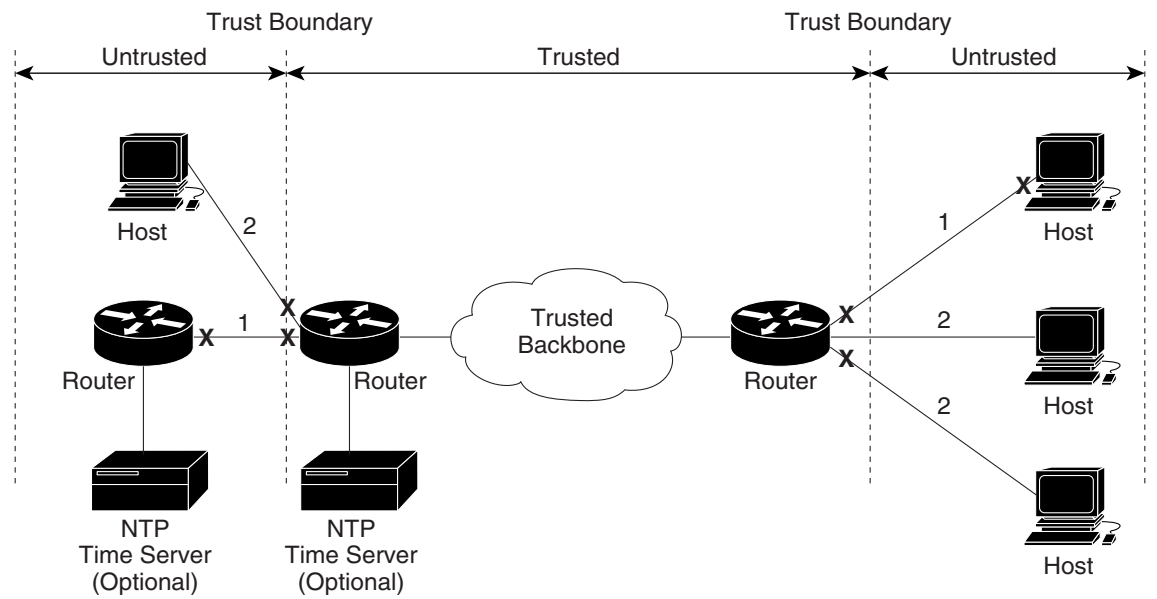
Network administrators need the ability to establish a security domain to control the set of systems that initiate RSVP requests.

The RSVP Message Authentication feature permits neighbors in an RSVP network to use a secure hash to sign all RSVP signaling messages digitally, thus allowing the receiver of an RSVP message to verify the sender of the message without relying solely on the sender's IP address as is done by issuing the **ip rsvp neighbor** command with an access control list (ACL).

The signature is accomplished on a per-RSVP-hop basis with an RSVP integrity object in the RSVP message. This method provides protection against forgery or message modification. However, the receiver must know the security key used by the sender in order to validate the digital signature in the received RSVP message.

Network administrators manually configure a common key for each RSVP neighbor interface on the shared network. A sample configuration is shown in [Figure 1](#).

Figure 1 *RSVP Message Authentication Configuration*

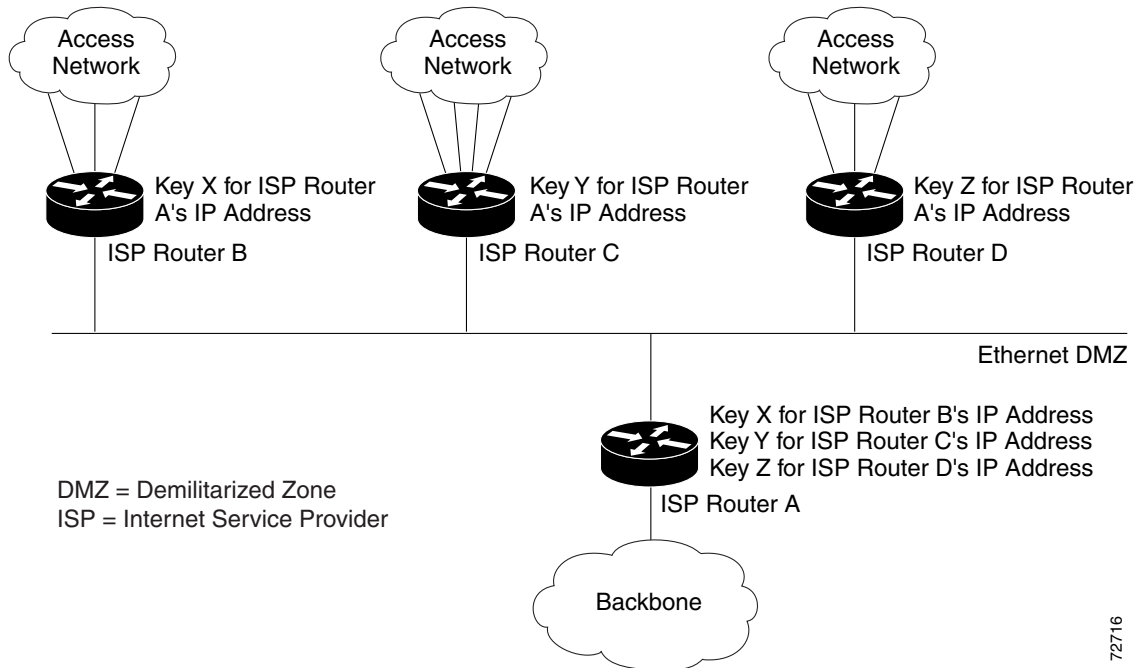


1 = Knows Authentication Key; Accepted
 2 = Does Not Know Key; Rejected
 X = RSVP Authentication Enabled

72677

Special Considerations for RSVP Message Authentication

Figure 2 RSVP Message Authentication in an Ethernet Configuration



In [Figure 2](#), to enable authentication between Internet service providers (ISPs) A and B, A and C, and A and D, the ISPs must share a common key. However, sharing a common key also enables authentication between ISPs B and C, C and D, and B and D. You may not want authentication among all the ISPs because they might be different companies with unique security domains.

This release does not support the above topology.

You need separate Ethernet networks for A to B, B to A, A to C, C to A, A to D, and D to A. Then configure unique interface keys for them.

Benefits of RSVP Message Authentication

Improved Security

The RSVP Message Authentication feature greatly reduces the chance of an RSVP-based spoofing attack and provides a secure method to control QoS access to a network.

Multiple Environments

The RSVP Message Authentication feature can be used in traffic engineering (TE) and non-TE environments as well as with subnetwork bandwidth manager (SBM).

Multiple Platforms and Interfaces

The RSVP Message Authentication feature can be used on any supported RSVP platform or interface.

How to Configure RSVP Message Authentication

The following configuration parameters instruct RSVP on how to generate and verify integrity objects in various RSVP messages.

**Note**

There are two configuration procedures—full and minimal.

This section contains the following procedures for a full configuration:

- [Enabling RSVP on an Interface, page 5](#) (required)
- [Configuring an RSVP Authentication Type, page 6](#) (optional)
- [Configuring an RSVP Authentication Key, page 7](#) (required)
- [Enabling RSVP Key Encryption, page 8](#) (optional)
- [Enabling RSVP Authentication Challenge, page 9](#) (optional)
- [Configuring RSVP Authentication Lifetime, page 10](#) (optional)
- [Configuring RSVP Authentication Window Size, page 11](#) (optional)
- [Activating RSVP Authentication, page 12](#) (required)
- [Verifying RSVP Message Authentication, page 13](#) (optional)

This section contains the following tasks for a minimal configuration:

- [Enabling RSVP on an Interface, page 5](#) (required)
- [Configuring an RSVP Authentication Key, page 7](#) (required)
- [Activating RSVP Authentication, page 12](#) (required)

Enabling RSVP on an Interface

Perform this task to enable RSVP on an interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *[type number]*
4. **ip rsvp bandwidth** *[interface-kbps]* *[single-flow-kbps]*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface [<i>type number</i>] Example: Router(config)# interface Ethernet0/0	Enters interface configuration mode. <ul style="list-style-type: none"> The <i>type number</i> argument identifies the interface to be configured.
Step 4	ip rsvp bandwidth [<i>interface-kbps</i>] [<i>single-flow-kbps</i>] Example: Router(config-if)# ip rsvp bandwidth 7500 7500	Enables RSVP on an interface. <ul style="list-style-type: none"> The optional <i>interface-kbps</i> and <i>single-flow-kbps</i> arguments specify the amount of bandwidth that can be allocated by RSVP flows or to a single flow, respectively. Values are from 1 to 10,000,000. <p>Note Repeat this command for each interface that you want to enable.</p>
Step 5	end Example: Router(config-if)# end	Exits to privileged EXEC mode.

Configuring an RSVP Authentication Type

Perform this task to configure an RSVP authentication type.

SUMMARY STEPS

- enable**
- configure terminal**
- interface** [*type number*]
- ip rsvp authentication type** {md5 | sha-1}
- end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface [<i>type number</i>] Example: Router(config)# interface Ethernet0/0	Enters interface configuration mode. <ul style="list-style-type: none"> The <i>type number</i> argument identifies the interface to be configured.
Step 4	ip rsvp authentication type { md5 sha-1 } Example: Router(config-if)# ip rsvp authentication type sha-1	Specifies the algorithm used to generate cryptographic signatures in RSVP messages. <ul style="list-style-type: none"> The algorithms are md5, the default, and sha-1, which is newer and more secure than md5.
Step 5	end Example: Router(config-if)# end	Exits to privileged EXEC mode.

Configuring an RSVP Authentication Key

Perform this task to configure an RSVP authentication key.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** [*type number*]
4. **ip rsvp authentication key** *passphrase*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface [<i>type number</i>] Example: Router(config)# interface Ethernet0/0	Enters interface configuration mode. <ul style="list-style-type: none"> The <i>type number</i> argument identifies the interface to be configured.
Step 4	ip rsvp authentication key <i>passphrase</i> Example: Router(config-if)# ip rsvp authentication key 11223344	Specifies the data string (key) for the authentication algorithm. <ul style="list-style-type: none"> The key consists of 8 to 40 characters. It can include spaces and multiple words. It can also be encrypted or appear in clear text when displayed.
Step 5	end Example: Router(config-if)# end	Exits to privileged EXEC mode.

Enabling RSVP Key Encryption

Perform this task to enable RSVP key encryption when the key is stored in the router configuration. (This prevents anyone from seeing the clear text key in the configuration file.)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key config-key 1** *string*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	key config-key 1 string Example: Router(config)# key config-key 1 11223344	Enables key encryption in the configuration file. <ul style="list-style-type: none"> The <i>string</i> argument can contain up to eight alphanumeric characters.
Step 4	end Example: Router(config)# end	Exits to privileged EXEC mode.

Enabling RSVP Authentication Challenge

Perform this task to enable RSVP authentication challenge.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** [*type number*]
4. **ip rsvp authentication challenge**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	interface [<i>type number</i>] Example: Router(config)# interface Ethernet0/0	Enters interface configuration mode. <ul style="list-style-type: none"> The <i>type number</i> argument identifies the interface to be configured.
Step 4	ip rsvp authentication challenge Example: Router(config-if)# ip rsvp authentication challenge	Makes RSVP perform a challenge-response handshake when RSVP learns about any new challenge-capable neighbors on a network.
Step 5	end Example: Router(config-if)# end	Exits to privileged EXEC mode.

Configuring RSVP Authentication Lifetime

Perform this task to configure the lifetimes of security associations between RSVP neighbors.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** [*type number*]
4. **ip rsvp authentication lifetime hh:mm:ss**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface [<i>type number</i>] Example: Router(config)# interface Ethernet0/0	Enters interface configuration mode. <ul style="list-style-type: none"> The <i>type number</i> argument identifies the interface to be configured.

	Command or Action	Purpose
Step 4	<pre>ip rsvp authentication lifetime hh:mm:ss</pre> <p>Example: Router(config-if)# ip rsvp authentication 00:05:00 </p>	Controls how long RSVP maintains security associations with RSVP neighbors. <ul style="list-style-type: none"> The default security association for hh:mm:ss is 30 minutes; the range is 1 second to 24 hours.
Step 5	<pre>end</pre> <p>Example: Router(config-if)# end </p>	Exits to privileged EXEC mode.

Configuring RSVP Authentication Window Size

Perform this task to configure RSVP authentication window size.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** [*type number*]
4. **ip rsvp authentication window-size** [*n*]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p>Example: Router> enable </p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<pre>configure terminal</pre> <p>Example: Router# configure terminal </p>	Enters global configuration mode.
Step 3	<pre>interface [type number]</pre> <p>Example: Router(config)# interface Ethernet0/0 </p>	Enters interface configuration mode. <ul style="list-style-type: none"> The <i>type number</i> argument identifies the interface to be configured.

	Command or Action	Purpose
Step 4	ip rsvp authentication window-size [n] Example: Router(config-if)# ip rsvp authentication window-size 2	Specifies the maximum number of authenticated messages that can be received out of order. <ul style="list-style-type: none"> The default value is one message; the range is 1 to 64 messages.
Step 5	end Example: Router(config-if)# end	Exits to privileged EXEC mode.

Activating RSVP Authentication

Perform this task to activate RSVP authentication.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** [type number]
4. **ip rsvp authentication**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface [type number] Example: Router(config)# interface Ethernet0/0	Enters interface configuration mode. <ul style="list-style-type: none"> The <i>type number</i> argument identifies the interface to be configured.

	Command or Action	Purpose
Step 4	<code>ip rsvp authentication</code> Example: Router(config-if)# ip rsvp authentication	Activates RSVP cryptographic authentication.
Step 5	<code>end</code> Example: Router(config-if)# end	Exits to privileged EXEC mode.

Verifying RSVP Message Authentication

Perform this task to verify that the RSVP Message Authentication feature is functioning.

SUMMARY STEPS

1. `enable`
2. `show ip rsvp interface [interface-type interface-number] [detail]`
3. `show ip rsvp authentication [detail] [ip-address | hostname]`
4. `show ip rsvp counters [interface interface_unit | summary | neighbor]`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<code>show ip rsvp interface [interface-type interface-number] [detail]</code> Example: Router# show ip rsvp interface detail	Displays information about interfaces on which RSVP is enabled, including the current allocation budget and maximum available bandwidth. <ul style="list-style-type: none"> • The optional detail keyword displays the bandwidth, signaling, and authentication parameters.

	Command or Action	Purpose
Step 3	<pre>show ip rsvp authentication [detail] [ip-address hostname]</pre> <p>Example: Router# show ip rsvp authentication detail</p>	<p>Displays the security associations that RSVP has established with other RSVP neighbors.</p> <ul style="list-style-type: none"> The optional detail keyword displays state information that includes IP addresses, interfaces enabled, and configured cryptographic authentication parameters about security associations that RSVP has established with neighbors.
Step 4	<pre>show ip rsvp counters [interface interface_unit summary neighbor]</pre> <p>Example: Router# show ip rsvp counters summary</p>	<p>(Optional) Displays the number of RSVP messages that were sent and received on each interface; shows error counter incrementing whenever an RSVP message is received on an interface with RSVP authentication enabled, but authentication checks failed on that message.</p> <p>Note The error counter can also increment when it receives an error not related to authentication.</p> <ul style="list-style-type: none"> The optional summary keyword shows the cumulative number of RSVP messages sent and received by the platform.

Examples

This section provides the following example output:

- [Sample Output for the show ip rsvp authentication detail Command, page 14](#)
- [Sample Output for the show ip rsvp interface detail Command, page 14](#)

Sample Output for the show ip rsvp authentication detail Command

In this example, the **show ip rsvp authentication detail** command displays information, including IP addresses, interfaces enabled, and configured cryptographic authentication parameters about security associations that RSVP has established with neighbors.

```
Router# show ip rsvp authentication detail

Neighbor: 192.168.101.2  Key ID (hex): 62d0b1140000
Interface: Ethernet0/0  Key type:   Static
Direction: Send        Expiration: 000d 00h 29m 39s
Last seq # sent:
13851245224380071944

Neighbor: 192.168.101.2  Key ID (hex): 62d164fc00000
Interface: Ethernet0/0  Key type:   Static
Direction: Receive     Expiration: 000d 00h 29m 39s
Last valid seq # rcvd:  Challenge:  Not configured
13851246177862811649
```

Sample Output for the show ip rsvp interface detail Command

In this example, the **show ip rsvp interface detail** command displays detailed information, including the cryptographic authentication parameters, for all RSVP-configured interfaces on a router.

**Note**

The authentication key in the following example appears encrypted (<encrypted>). That is because the **key config-key 1 string** command was issued prior to the **show ip rsvp interface detail** command.

```
Router# show ip rsvp interface detail

Et0/0:
  Bandwidth:
    Curr allocated: 0 bits/sec
    Max. allowed (total): 7500K bits/sec
    Max. allowed (per flow): 7500K bits/sec
    Max. allowed for LSP tunnels using sub-pools: 0 bits/sec
    Set aside by policy (total):0 bits/sec
  Neighbors:
    Using IP encap: 0. Using UDP encap: 0
  Signalling:
    Refresh reduction: disabled
  Authentication: enabled
  Key:               <encrypted>
  Type:              sha-1
  Window size:      2
  Challenge:         enabled
```

Troubleshooting Tips

To troubleshoot the RSVP Message Authentication feature, use the following commands in privileged EXEC mode:

Command	Purpose
Router# debug ip rsvp authentication	Displays output related to RSVP authentication.
Router# debug ip rsvp dump signalling	Displays brief information about signaling (Path and Resv) messages.

Configuration Examples for RSVP Message Authentication

This section provides the following configuration example:

- [RSVP Message Authentication Example, page 16](#)

RSVP Message Authentication Example

In the following output, the cryptographic authentication parameters, including type, key, challenge, lifetime, window size, are configured; and authentication is activated:

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# interface e0/0

Router(config-if)# ip rsvp bandwidth 7500 7500

Router(config-if)# ip rsvp authentication type sha-1

Router(config-if)# ip rsvp authentication key 11223344

Router(config-if)# ip rsvp authentication challenge

Router(config-if)# ip rsvp authentication lifetime 00:30:05

Router(config-if)# ip rsvp authentication window-size 2

Router(config-if)# ip rsvp authentication
```

In the following output from the **show ip rsvp interface detail** command, notice the cryptographic authentication parameters that you configured for the Ethernet0/0 interface:

```
Router# show ip rsvp interface detail

Et0/0:
  Bandwidth:
    Curr allocated: 0 bits/sec
    Max. allowed (total): 7500K bits/sec
    Max. allowed (per flow): 7500K bits/sec
    Max. allowed for LSP tunnels using sub-pools: 0 bits/sec
    Set aside by policy (total): 0 bits/sec
  Neighbors:
    Using IP encap: 0. Using UDP encap: 0
  Signalling:
    Refresh reduction: disabled
  Authentication: enabled
    Key:          11223344
    Type:         sha-1
    Window size: 2
    Challenge:    enabled
```

In the preceding example, the authentication key appears in clear text. If you enter the **key-config-key 1 string** command, the key appears encrypted, as in the following example:

```
Router# show ip rsvp interface detail

Et0/0:
```

```
Bandwidth:
  Curr allocated: 0 bits/sec
Max. allowed (total): 7500K bits/sec
  Max. allowed (per flow): 7500K bits/sec
  Max. allowed for LSP tunnels using sub-pools: 0 bits/sec
  Set aside by policy (total): 0 bits/sec
Neighbors:
  Using IP encap: 0. Using UDP encap: 0
Signalling:
  Refresh reduction: disabled
Authentication: enabled
  Key: <encrypted>
  Type: sha-1
  Window size: 2
  Challenge: enabled
```

In the following output, notice the authentication key changes from encrypted to clear text after the **no key config-key 1** command is issued:

```
Router# show run int e0/0

Building configuration...

Current configuration :247 bytes
!
interface Ethernet0/0
 ip address 192.168.101.2 255.255.255.0
 no ip directed-broadcast
 ip pim dense-mode
 no ip mroute-cache
 no cdp enable
 ip rsvp bandwidth 7500 7500
 ip rsvp authentication key 7>70>9:7<872>?74
 ip rsvp authentication
end

Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# no key config-key 1

Router(config)# end

Router# show run
*Jan 30 08:02:09.559:%SYS-5-CONFIG_I:Configured from console by console
int e0/0
Building configuration...

Current configuration :239 bytes
!
interface Ethernet0/0
 ip address 192.168.101.2 255.255.255.0
 no ip directed-broadcast
 ip pim dense-mode
 no ip mroute-cache
 no cdp enable
 ip rsvp bandwidth 7500 7500
 ip rsvp authentication key 11223344
 ip rsvp authentication
end
```

Additional References

For additional information related to the RSVP Message Authentication feature, refer to the following references:

- [Related Documents, page 18](#)
- [Standards, page 18](#)
- [MIBs, page 18](#)
- [RFCs, page 19](#)
- [Technical Assistance, page 19](#)

Related Documents

Related Topic	Document Title
RSVP commands: complete command syntax, command mode, defaults, usage guidelines, and examples	Cisco IOS Quality of Service Solutions Command Reference, Release 12.2
QoS features including signaling, classification, and congestion management	Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2
Error messages	Cisco IOS System Error Messages

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing standards has not been modified by this feature.	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

RFCs ¹	Title
RFC 1321	<i>The MD5 Message Digest Algorithm</i>
RFC 2104	<i>HMAC: Keyed-Hashing for Messaging Authentication</i>
RFC 2205	<i>Resource Reservation Protocol</i>
RFC 2209	<i>RSVP—Version 1 Message Processing Rules</i>
RFC 2401	<i>Security Architecture for the Internet Protocol</i>
RFC 2747	<i>RSVP Cryptographic Authentication</i>
RFC 3174	<i>US Secure Hash Algorithm 1 (SHA1)</i>

1. Not all supported RFCs are listed.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

New Commands

- **clear ip rsvp authentication**
- **debug ip rsvp authentication**
- **ip rsvp authentication**
- **ip rsvp authentication challenge**
- **ip rsvp authentication key**
- **ip rsvp authentication lifetime hh:mm:ss**
- **ip rsvp authentication type**
- **ip rsvp authentication window-size**
- **show ip rsvp authentication**

Modified Commands

- **show ip rsvp counters**
- **show ip rsvp interface**

clear ip rsvp authentication

To eliminate Resource Reservation Protocol (RSVP) security associations before their lifetimes expire, use the **clear ip rsvp authentication** command in EXEC mode.

clear ip rsvp authentication [*ip-address* | *hostname*]

Syntax Description

<i>ip-address</i>	(Optional) Frees security associations with a specific neighbor.
<i>hostname</i>	(Optional) Frees security associations with a specific host.



Note

The difference between *ip-address* and *hostname* is whether you specify the neighbor by its ip address or by its name.

Defaults

Clear all associations.

Command Modes

EXEC

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use the **clear ip rsvp authentication** command for the following reasons:

- To eliminate security associations before their lifetimes expire
- To free up memory
- To resolve a problem with a security association being in some indeterminate state
- To force reauthentication of neighbors

You can delete all RSVP security associations if you do not enter an IP address or a host name, or just the ones with a specific RSVP neighbor or host.

If you delete a security association, it is re-created as needed when the trusted RSVP neighbors start sending more RSVP messages.

Examples

The following command shows how to clear all security associations before they expire:

```
Router# clear ip rsvp authentication
```

■ clear ip rsvp authentication

Related Commands

Command	Description
ip rsvp authentication lifetime hh:mm:ss	Controls how long RSVP maintains security associations with other trusted RSVP neighbors.
show ip rsvp authentication	Displays security associations established with neighbors.

debug ip rsvp authentication

To display debug output related to Resource Reservation Protocol (RSVP) authentication, use the **debug ip rsvp authentication** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ip rsvp authentication

no debug ip rsvp authentication

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

After you enable RSVP authentication, RSVP logs system error events whenever an authentication check fails. These events are logged instead of just being displayed when debugging is enabled because they may indicate potential security attacks. The events are generated when:

- RSVP receives a message that does not contain the correct cryptographic signature. This could be due to misconfiguration of the authentication key or algorithm on one or more RSVP neighbors, but it may also indicate an (unsuccessful) attack.
- RSVP receives a message with the correct cryptographic signature, but with a duplicate authentication sequence number. This may indicate an (unsuccessful) message replay attack.
- RSVP receives a message with the correct cryptographic signature, but with an authentication sequence number that is outside the receive window. This could be due to a reordered burst of valid RSVP messages, but it may also indicate an (unsuccessful) message replay attack.
- Failed challenges result from timeouts or bad challenge responses.

Examples

The following example shows output from the **debug ip rsvp authentication** command in which the authentication type (digest) and the sequence number have been validated:

```
Router# debug ip rsvp authentication
```

```
RSVP authentication debugging is on
```

```
Router# show debugging
```

```
*Jan 30 08:10:46.335:RSVP_AUTH:Resv integrity digest from 192.168.101.2 valid
```

```
*Jan 30 08:10:46.335:RSVP_AUTH:Resv integrity sequence number 13971113505298841601 from 192.168.101.2 valid
```

*Jan 30 08:10:46.335:RSVP_AUTH:Resv from 192.168.101.2 passed all authentication checks

**Note**

Cisco routers using RSVP authentication on Cisco IOS ideally should have clocks that can be accurately restored to the correct time when the routers boot. This capability is available on certain Cisco routers that have clocks with battery backup. For those platforms that do not have battery backup, consider configuring the router to keep its clock synchronized with a Network Time Protocol (NTP) time server. Otherwise, if two adjacent routers have been operating with RSVP authentication enabled and one of them reboots such that its clock goes backward in time, it is possible (but unlikely) the router that did not reboot will log RSVP authentication sequence number errors.

Related Commands

Command	Description
ip rsvp authentication	Activates RSVP cryptographic authentication.
show debug	Displays active debug output.

ip rsvp authentication

To activate Resource Reservation Protocol (RSVP) cryptographic authentication, use the **ip rsvp authentication** command in interface configuration mode. To deactivate authentication, use the **no** form of this command.

ip rsvp authentication

no ip rsvp authentication

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use the **ip rsvp authentication** command to deactivate and then reactivate RSVP authentication without reentering the other RSVP authentication configuration commands. You should not enable authentication unless you have previously configured a key. If you issue this command before the **ip rsvp authentication key** command, you get a warning message indicating that RSVP discards all messages until you specify a key. The **no ip rsvp authentication** command disables RSVP cryptographic authentication. However, the command does not automatically remove any other authentication parameters that you have configured. You must issue a specific **no ip rsvp authentication** command; for example, **no ip rsvp authentication key**, **no ip rsvp authentication type**, or **no ip rsvp authentication window-size**, if you want to remove them from the configuration.

The **ip rsvp authentication** command is similar to the **ip rsvp neighbor** command. However, the **ip rsvp authentication** command provides better authentication and performs system logging.

Examples

The following command activates authentication on an interface:

```
Router(config-if)# ip rsvp authentication
```

The following command deactivates authentication on an interface:

```
Router(config-if)# no ip rsvp authentication
```

■ ip rsvp authentication

Related Commands	Command	Description
	ip rsvp authentication key	Specifies the key for the authentication algorithm.
	ip rsvp neighbor	Enables neighbors to request a reservation.

ip rsvp authentication challenge

To make Resource Reservation Protocol (RSVP) perform a challenge-response handshake with any new RSVP neighbors on a network, use the **ip rsvp authentication challenge** command in interface configuration mode. To disable the challenge-response handshake, use the **no** form of this command.

ip rsvp authentication challenge

no ip rsvp authentication challenge

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

The **ip rsvp authentication challenge** command requires RSVP to perform a challenge-response handshake with any new RSVP neighbors that are discovered on a network. Such a handshake allows the router to thwart RSVP message replay attacks while booting, especially if there is a long period of inactivity from trusted RSVP neighbors following the reboot. If messages from trusted RSVP neighbors arrive very quickly after the router reboots, then challenges may not be required because the router will have reestablished its security associations with the trusted nodes before the untrusted nodes can attempt replay attacks.

If you enable RSVP authentication challenges, you should consider enabling RSVP refresh reduction by using the **ip rsvp signalling refresh reduction** command. While a challenge handshake is in progress, the receiving router initiating the handshake discards all RSVP messages from the node being challenged until the handshake-initiating router receives a valid challenge response.



Note

If a neighbor does not reply to the first challenge message after 1 second, Cisco IOS sends another challenge message and waits 2 seconds. If no response is received to the second challenge, Cisco IOS sends another and waits 4 seconds. If no response to the third challenge is received, Cisco IOS sends a fourth challenge and waits 8 seconds. If there is no response to the fourth challenge, Cisco IOS stops the current challenge to that neighbor, logs a system error message, and does not create a security association for that neighbor. This kind of exponential backoff is used to recover from challenges dropped by the network or busy neighbors.

Activating refresh reduction enables the challenged node to resend dropped messages more quickly once the handshake has completed. This causes RSVP to reestablish reservation state faster when the router reboots.

Enable authentication challenges wherever possible to reduce the router's vulnerability to replay attacks.

Examples

The following command shows how to enable RSVP to perform a challenge-response handshake:

```
Router(config-if)# ip rsvp authentication challenge
```

Related Commands

Command	Description
ip rsvp signalling refresh reduction	Enables refresh reduction.

ip rsvp authentication key

To specify the key (string) for the Resource Reservation Protocol (RSVP) authentication algorithm, use the **ip rsvp authentication key** command in interface configuration mode. To disable the key, use the **no** form of this command.

ip rsvp authentication key *passphrase*

no ip rsvp authentication key

Syntax Description

<i>passphrase</i>	A range from 8 to 40 characters. See “Usage Guidelines” for additional information.
-------------------	---

Defaults

This command has no default key.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use the **ip rsvp authentication key** command to select the key for the authentication algorithm. This key is a passphrase of 8 to 40 characters. It can include spaces; quotes are not required if spaces are used. The key can consist of more than one word. We recommend that you make the passphrase as long as possible. This key must be the same for all RSVP neighbors on this interface. As with all passwords, you should choose them carefully so that attackers cannot easily guess them.

Here are some guidelines:

- Use a mixture of upper- and lowercase letters, digits, and punctuation.
- If using just a single word, do not use a word contained in any dictionary of any language, spelling lists, or other lists of words.
- Use something easily remembered so you do not have to write it down.
- Do not let it appear in clear text in any file or script or on a piece of paper attached to a terminal.

By default, RSVP authentication keys are stored in clear text in the router configuration file, but they can optionally be stored as encrypted text in the configuration file. To enable key encryption, use the global Cisco IOS configuration command **key config-key 1** *string*. After you enter this command, the passphrase parameter of each **ip rsvp authentication key** command is encrypted with the Data Encryption Standard (DES) algorithm when you save the configuration file. If you later issue a **no key config-key 1** *string* command, the RSVP authentication key is stored in clear text again when you save the configuration.

The *string* is not stored in the configuration file; it is stored only in the router's private nonvolatile random-access memory (NVRAM) and will not appear in the output of a **show run** or **show config** command. Therefore, if you copy the configuration file to another router, any encrypted RSVP keys in that file will not be successfully decrypted by RSVP when the router boots and RSVP authentication will not operate correctly. To recover from this, follow these steps on the new router:

1. For each RSVP interface with an authentication key, issue a **no ip rsvp authentication key** command to clear the old key.
2. For that same set of RSVP interfaces, issue an **ip rsvp authentication key** command to reconfigure the correct clear text keys.
3. Issue a global **key config-key 1 string** command to reencrypt the RSVP keys for the new router.
4. Save the configuration.

Examples

The following command sets the passphrase to 11223344 in clear text:

```
Router(config-if)# ip rsvp authentication key 11223344
```

To encrypt the authentication key, issue the **key config-key 1 string** command as follows:

```
Router# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)# key config-key 1 11223344
```

```
Router(config)# end
```

Related Commands

Command	Description
key config-key 1	Enables key encryption.

ip rsvp authentication lifetime hh:mm:ss

To control how long Resource Reservation Protocol (RSVP) maintains security associations with other trusted RSVP neighbors, use the **ip rsvp authentication lifetime hh:mm:ss** command in interface configuration mode. To disable the lifetime setting, use the **no** form of this command.

ip rsvp authentication lifetime hh:mm:ss

no ip rsvp authentication lifetime hh:mm:ss

Syntax Description

This command has no arguments or keywords.

Defaults

Default security association is 30 minutes; range is 1 second to 24 hours.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use the **ip rsvp authentication lifetime hh:mm:ss** command to indicate when to end security associations with RSVP trusted neighbors. If an association's lifetime expires, but at least one valid, RSVP authenticated message was received in that time period, RSVP resets the security association's lifetime to this configured value. When a neighbor stops sending RSVP signaling messages (that is, the last reservation has been torn down), the memory used for the security association is freed as well as when the association's lifetime period ends. The association can be re-created if that RSVP neighbor resumes its signaling. Setting the lifetime to shorter periods allows memory to be recovered faster when the router is handling a lot of short-lived reservations. Setting the lifetime to longer periods reduces the workload on the router when establishing new authenticated reservations.

Use the **clear ip rsvp authentication** command to free security associations before their lifetimes expire.

Examples

The following command sets the lifetime period for 30 minutes and 5 seconds:

```
Router(config-if)# ip rsvp authentication lifetime 00:30:05
```

Related Commands

Command	Description
clear ip rsvp authentication	Eliminates security associations before their lifetimes expire.

ip rsvp authentication type

To specify the algorithm to generate cryptographic signatures in Resource Reservation Protocol (RSVP) messages, use the **ip rsvp authentication type** command in interface configuration mode. To disable the type (or to use the default type, **md5**), use the **no** form of this command.

ip rsvp authentication type { md5 | sha-1 }

no ip rsvp authentication type

Syntax Description

md5	RSA Message Digest 5 algorithm.
sha-1	National Institute of Standards and Technologies (NIST) Secure Hash Algorithm-1; it is newer and more secure than md5.

Defaults

The default type is **md5**.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use the **ip rsvp authentication type** command to specify the algorithm to generate cryptographic signatures in RSVP messages. If you do not specify an algorithm, **md5** is used.

Examples

The following command sets the type to **sha-1**:

```
Router(config-if)# ip rsvp authentication type sha-1
```

Related Commands

Command	Description
ip rsvp authentication key	Specifies the key for the authentication algorithm.

ip rsvp authentication window-size

To specify the maximum number of Resource Reservation Protocol (RSVP) authenticated messages that can be received out of order, use the **ip rsvp authentication window-size** command in interface configuration mode. To disable the window-size (or to use the default value of 1), use the **no** form of this command.

ip rsvp authentication window-size [*n*]

no ip rsvp authentication window-size

Syntax Description	<i>n</i>	Maximum number of authenticated messages that can be received out of order. The range is 1 to 64.
---------------------------	----------	---

Defaults	The default value is one message.
-----------------	-----------------------------------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	12.2(15)T	This command was introduced.

Usage Guidelines	<p>Use the ip rsvp authentication window-size command to specify the maximum number of authenticated messages that can be received out of order. All RSVP authenticated messages include a sequence number that is used to prevent replays of RSVP messages.</p> <p>With a default window size of one message, RSVP rejects any duplicate authenticated messages because they are assumed to be replay attacks. However, sometimes bursts of RSVP messages become reordered between RSVP neighbors. If this occurs on a regular basis, and you can verify that the node sending the burst of messages is trusted, you can use the window-size option to allow for the burst size such that RSVP will not discard such reordered bursts. RSVP will still check for duplicate messages within these bursts.</p>
-------------------------	---

Examples	<p>The following command sets the window size to 2:</p> <pre>Router(config-if)# ip rsvp authentication window-size 2</pre>
-----------------	--

Related Commands	Command	Description
	ip rsvp authentication	Activates RSVP cryptographic authentication.

show ip rsvp authentication

To display the security associations that Resource Reservation Protocol (RSVP) has established with other RSVP neighbors, use the **show ip rsvp authentication** command in EXEC mode.

show ip rsvp authentication [detail] [*ip-address* | *hostname*]

Syntax Description

detail	(Optional) Additional information about RSVP security associations.
<i>ip-address</i>	(Optional) Information about a neighbor with a specified IP address.
<i>hostname</i>	(Optional) Information about a particular host.



Note

The difference between *ip-address* and *hostname* is whether you specify the neighbor by its ip address or by its name.

Command Modes

EXEC

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use the **show ip rsvp authentication** command to display the security associations that RSVP has established with other RSVP neighbors. You can display all security associations or specify an IP address or hostname of a particular RSVP neighbor, which restricts the size of the display.

Examples

The following example shows sample output from the **show ip rsvp authentication** command:

```
Router# show ip rsvp authentication

Neighbor      Interface Key Type   Key ID (hex) Direction Expiration
192.168.101.2 Et2/1     Static   62d0b1140000 Send      000d 00h 29m 46s
192.168.101.2 Et2/1     Static   62d164fc0000 Receive   000d 00h 29m 49s
```

The following example shows sample output from the **show ip rsvp authentication detail** command:

```
Router# show ip rsvp authentication detail

Neighbor: 192.168.101.2 Key ID (hex): 62d0b1140000
Interface: Ethernet0/0 Key type: Static
Direction: Send        Expiration: 000d 00h 29m 39s
Last seq # sent:
13851245224380071944

Neighbor: 192.168.101.2 Key ID (hex): 62d164fc0000
Interface: Ethernet0/0 Key type: Static
Direction: Receive     Expiration: 000d 00h 29m 39s
Last valid seq # rcvd: Challenge: Not configured
```

Table 1 describes the fields shown in the display.

Table 1 *show ip rsvp authentication detail Field Descriptions*

Field	Description
Neighbor	IP address of the RSVP neighbor with which the security association is being maintained.
Key ID	A string which, along with the IP address, uniquely identifies a security association. The key ID is automatically generated on Cisco IOS, but it may be configurable on other RSVP platforms. A key ID is provided in every RSVP authenticated message initiated by a sender and is stored by every RSVP receiver.
Interface	Name of the interface over which the security association is being maintained.
Key type	Static (manually configured). Note Cisco IOS software currently supports only static keys configured with the ip rsvp authentication key command. Cisco IOS software does not yet support RSVP neighbors that use dynamic keys.
Direction	Separate associations maintained for sending and receiving RSVP messages for a specific RSVP neighbor. Possible values are Send or Receive .
Expiration	Amount of time remaining (in days, hours, minutes, and seconds) before the security association expires.
Last seq # sent	Displayed only for send-type security associations. It indicates the sequence number used to send the last authenticated message to the RSVP neighbor. Use this information to troubleshoot certain types of authentication problems.
Last valid seq # rcvd	Displayed only for receive-type security associations. It indicates the authentication sequence number of the last valid RSVP message received from the neighbor. By default, it shows only one sequence number. However, if you use the ip rsvp authentication window-size command to increase the authentication window size to n , then the last n valid received sequence numbers are displayed. Use this information to troubleshoot certain types of authentication problems.
Challenge	Displayed only for receive-type security associations. Possible values are Not configured, Completed, In progress, and Failed.

Related Commands

Command	Description
clear ip rsvp authentication	Eliminates security associations before their lifetimes expire.

show ip rsvp counters

To display the number of Resource Reservation Protocol (RSVP) messages that were sent and received on each interface, use the **show ip rsvp counters** command in EXEC mode.

show ip rsvp counters [**interface** *interface_unit* | **summary** | **neighbor**]

Syntax Description	interface <i>interface_unit</i> (Optional) Number of RSVP messages sent and received for the specified interface name.
	summary (Optional) Cumulative number of RSVP messages sent and received by the platform.
	neighbor (Optional) Number of RSVP messages sent and received by the specified neighbor.

Defaults If you enter the **show ip rsvp counters** command without a keyword, the command displays the number of RSVP messages that were sent and received for each interface on which RSVP is configured.

Command Modes EXEC

Command History	Release	Modification
	12.0(14)ST	This command was introduced.
	12.2(15)T	The neighbor keyword was added and the output was modified to show the errors counter incrementing whenever an RSVP message is received on an interface with RSVP authentication enabled, but the authentication checks failed on that message.

Usage Guidelines Use the **show ip rsvp counters** command to display the number of RSVP messages that were sent and received for each interface on which RSVP is configured.

Examples The following command shows values for the number of RSVP messages of each type that were sent and received by the router over all interfaces:

```
Router# show ip rsvp counters summary
```

All Interfaces	Recv	Xmit		Recv	Xmit
Path	32	0	Resv	0	18
PathError	0	0	ResvError	0	0
PathTear	3	0	ResvTear	0	1
ResvConf	0	0	RTearConf	0	0
Ack	0	0	Srefresh	0	0
IntegrityChalle	0	0	IntegrityRespon	0	0
DSBM_WILLING	0	0	I_AM_DSBM	0	0
Unknown	0	0	Errors	12	0

Table 2 describes the fields shown in the display.

Table 2 *show ip rsvp counters Field Descriptions*

Field	Description
All Interfaces	Number of messages displayed for all interfaces.
Recv	Number of messages received at the specified interface or at all interfaces.
Xmit	Number of messages transmitted from the specified interface or from all interfaces.

Related Commands

Command	Description
clear ip rsvp counters	Clears (sets to zero) all IP RSVP counters that are being maintained.

show ip rsvp interface

To display Resource Reservation Protocol (RSVP)-related interface information, use the **show ip rsvp interface** command in EXEC mode.

show ip rsvp interface [*interface-type interface-number*] [**detail**]

Syntax Description		
	<i>interface-type</i>	(Optional) Type of the interface.
	<i>interface-number</i>	(Optional) Number of the interface.
	detail	(Optional) Additional information about interfaces.

Command Modes EXEC

Command History	Release	Modification
	11.2	This command was introduced.
	12.2(2)T	The detail keyword was added.
	12.2(15)T	Cryptographic authentication parameters were added to the display.

Usage Guidelines Use the **show ip rsvp interface** command to display information about interfaces on which RSVP is enabled, including the current allocation budget and maximum available bandwidth. Enter the optional **detail** keyword for additional information, including the cryptographic authentication parameters.

Examples The following command displays detailed information, including the cryptographic authentication parameters, for all RSVP-configured interfaces on the router:

```
Router# show ip rsvp interface detail

Et0/0:
  Bandwidth:
    Curr allocated: 0 bits/sec
    Max. allowed (total): 7500K bits/sec
    Max. allowed (per flow): 7500K bits/sec
    Max. allowed for LSP tunnels using sub-pools: 0 bits/sec
    Set aside by policy (total):0 bits/sec
  Neighbors:
    Using IP encap: 0.   Using UDP encap: 0
  Signalling:
    Refresh reduction: disabled
  Authentication: enabled
  Key:              11223344
  Type:             sha-1
  Window size:     2
  Challenge:       enabled
```

Table 3 describes the significant fields shown in the display.

Table 3 *show ip rsvp interface detail Field Descriptions*

Field	Description
Et0/0	Interface name.
Bandwidth	The RSVP bandwidth parameters in effect including the following: <ul style="list-style-type: none"> • Curr allocated = amount of bandwidth currently allocated in bits per second. • Max. allowed (total) = maximum amount of bandwidth allowed in bits per second. • Max. allowed (per flow) = maximum amount of bandwidth allowed per flow in bits per second. • Max. allowed for LSP tunnels using sub-pools = maximum amount of bandwidth allowed for label switched path (LSP) tunnels in bits per second. • Set aside by policy (total) = the amount of bandwidth set aside by the local policy in bits per second.
Neighbors	The number of neighbors using IP and UDP encapsulation.
Signalling	The type of signaling in effect; Refresh reduction is either enabled (active) or disabled (inactive).
Authentication	Authentication is either enabled (active) or disabled (inactive). The parameters include the following: <ul style="list-style-type: none"> • Key = The key (string) for the RSVP authentication algorithm displayed in clear text (for example, 11223344) or encrypted <encrypted>. • Type = The algorithm to generate cryptographic signatures in Resource Reservation Protocol (RSVP) messages; possible values are md5 and sha-1. • Window size = Maximum number of RSVP authenticated messages that can be received out of order. • Challenge = The challenge-response handshake performed with any new RSVP neighbors that are discovered on a network; possible values are enabled (active) or disabled (inactive).

Related Commands

Command	Description
<code>show ip rsvp neighbor</code>	Displays current RSVP neighbors.

Glossary

admission control—The process in which an RSVP reservation is accepted or rejected based on end-to-end available network resources.

bandwidth—The difference between the highest and lowest frequencies available for network signals. The term also is used to describe the rated throughput capacity of a given network medium or protocol.

DMZ—demilitarized zone. The neutral zone between public and corporate networks.

flow—A stream of data traveling between two endpoints across a network (for example, from one LAN station to another). Multiple flows can be transmitted on a single circuit.

key—A data string that is combined with source data according to an algorithm to produce output that is unreadable until decrypted.

QoS—quality of service. A measure of performance for a transmission system that reflects its transmission quality and service availability.

router—A network layer device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another based on network layer information.

RSVP—Resource Reservation Protocol. A protocol that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so on) of the packet streams they want to receive.

security association—A block of memory used to hold all the information RSVP needs to authenticate RSVP signaling messages from a specific RSVP neighbor.

spoofing—The act of a packet illegally claiming to be from an address from which it was not actually sent. Spoofing is designed to foil network security mechanisms, such as filters and access lists.

trusted neighbor—A router with authorized access to information.

VoIP—Voice over IP. The ability to carry normal telephony-style voice over an IP-based Internet maintaining telephone-like functionality, reliability, and voice quality.