RSVP-Previous Hop Overwrite

Last Updated: October 11, 2012

The RSVP--Previous Hop Overwrite feature allows you to configure a Resource Reservation Protocol (RSVP) device, on a per interface basis, to populate an address other than the native interface address in the previous hop (PHOP) address field of the PHOP object when forwarding a PATH message onto that interface. You can configure the actual address for the device to use or an interface, including a loopback, from which to borrow the address.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for RSVP-Previous Hop Overwrite

You must configure RSVP on one or more interfaces on at least two neighboring devices that share a link within the network.

Restrictions for RSVP-Previous Hop Overwrite

- This feature is supported only on integrated services routers (ISRs).
- Unnumbered IP addresses are not allowed.

Information About RSVP-Previous Hop Overwrite

Feature Overview of RSVP-Previous Hop Overwrite

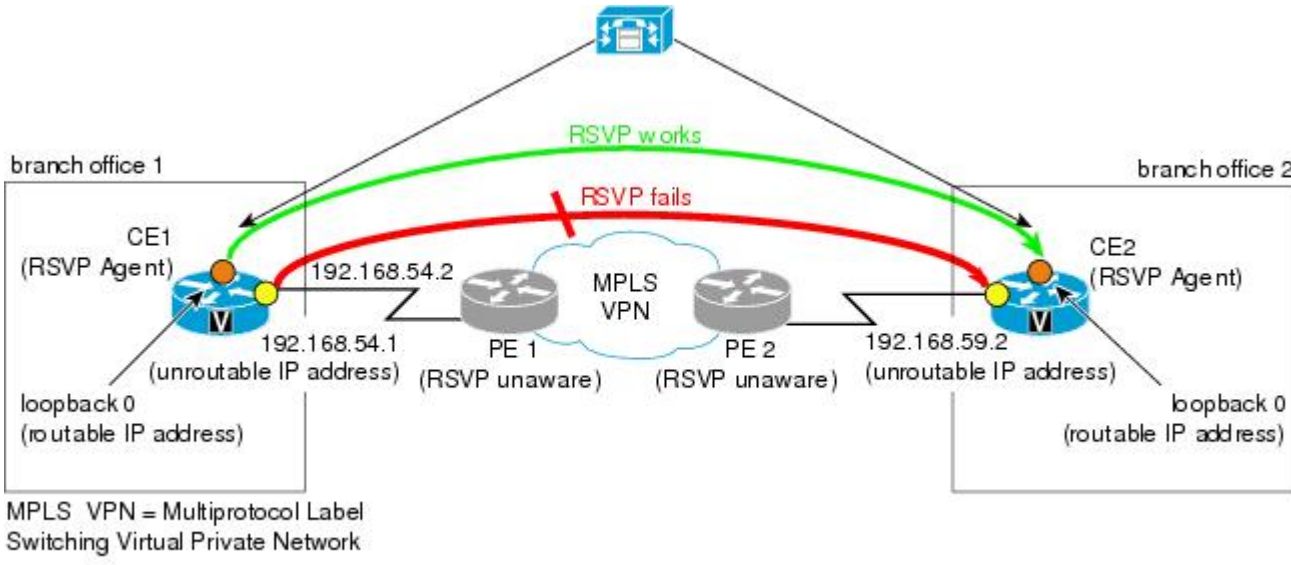
An RSVP PATH message contains a PHOP object that is rewritten at every RSVP hop. The object's purpose is to enable an RSVP device (R1) sending a PATH message to convey to the next RSVP device (R2) downstream that the previous RSVP hop is R1. R2 uses this information to forward the corresponding RESV message upstream hop-by-hop towards the sender.

The current behavior in Cisco software is that an RSVP device always sets the PHOP address to the IP address of the egress interface onto which the device transmits the PATH message.

There are situations where, although some IP addresses of R1 are reachable, the IP address of its egress interface is not reachable from a remote RSVP device R2. This results in the corresponding RESV message generated by R2 never reaching R1 and the reservation never being established.

The figure below shows a sample network in which the preceding scenario occurs and no reservation is established.

Figure 1 Sample PHOP Network with Unified Communcations Manager (CM)



In the figure above, when a call is made from branch office 1 to branch office 2, the RSVP Agent on customer edge (CE)1 tries to set up a session with CE2 and sends a PATH message. CE1 stamps its outgoing interface IP address (192.168.54.1), which is an unroutable IP address, in the PHOP object of the PATH message. This PATH message is tunneled across the service provider network and processed by CE2. CE2 records this IP address in the PHOP object of the received PATH message in the PSB (Path State Block).

CE2 has a receiver proxy configured for the destination address of the session. As a result, when CE2 replies back with a RESV message, CE2 tries to send the RESV message to the IP address that CE2 had recorded in its PSB. Because this IP address (192.168.54.1) is unroutable from CE2, the RESV message will fail.

Note Once you configure a source address on an interface, RSVP always uses the RSVP-overwritten address rather than the native interface address.

Benefits of RSVP-Previous Hop Overwrite

Flexibility and Customization

You can configure a CE to populate the PHOP object in a PATH message with an address that is reachable in the customer VPN. This enables the RESV message to find its way back towards the sender so that reservations can be established.

How to Configure RSVP-Previous Hop Overwrite

Configuring a Source Address or a Source Interface

Perform this task to configure a source address or a source interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip rsvp bandwidth** [*interface-kbps*] [*single-flow-kbps*]
5. **ip rsvp source** {**address** *ip-address* | **interface** *type number*}
6. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface Ethernet0/0`	Configures the interface type and enters interface configuration mode.
Step 4	**ip rsvp bandwidth** [*interface-kbps*] [*single-flow-kbps*] **Example:** `Device(config-if)# ip rsvp bandwidth`	Enables RSVP on an interface. • The optional *interface-kbps* and *single-flow-kbps* arguments specify the amount of bandwidth that can be allocated by RSVP flows or to a single flow, respectively. Values are from 1 to 10000000. **Note** Repeat this command for each interface on which you want to enable RSVP.
Step 5	**ip rsvp source** {**address** *ip-address* | **interface** *type number*} **Example:** `Device(config-if)# ip rsvp source` **address 10.1.3.13**	Configures an RSVP device to populate an address other than the native interface address in the PHOP address field of the hop object when forwarding a PATH message onto that interface. **Note** The source IP address that you configure should be a valid local IP address.
Step 6	end **Example:** `Device(config-if)# end`	(Optional) Returns to privileged EXEC mode.

Verifying the PHOP Configuration

Note You can use the following **show** command in user EXEC or privileged EXEC mode.

SUMMARY STEPS

1. **enable**
2. **show ip rsvp interface** [**detail**] [*interface-type interface-number*]
3. **exit**

DETAILED STEPS

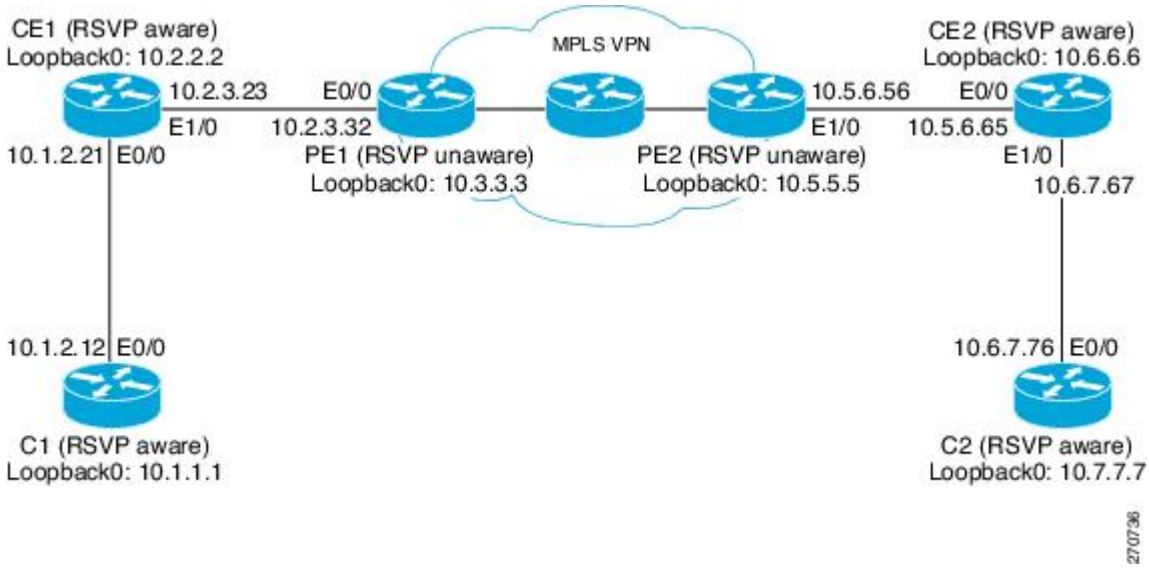
	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	(Optional) Enables privileged EXEC mode. • Enter your password if prompted. **Note** Skip this step if you are using the **show** command in user EXEC mode.
Step 2	**show ip rsvp interface** [**detail**] [*interface-type interface-number*] **Example:** `Device# show ip rsvp interface detail ethernet0/1`	(Optional) Displays RSVP-related interface information. • The optional keywords and arguments display additional information.
Step 3	**exit** **Example:** `Device# exit`	(Optional) Exits privileged EXEC mode and returns to user EXEC mode.

Configuration Examples for RSVP-Previous Hop Overwrite

Examples Configuring RSVP-Previous Hop Overwrite

The figure below shows a sample network in which PHOP is configured.

Figure 2 Sample PHOP Network



Configuring a Source Address on Device CE1 for the CE1-to-PE1 Interface

The following example configures a source address on the CE1-to-PE1 (Ethernet 1/0) interface in the figure above:

```
Device(CE1)# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Device(CE1)(config)# interface ethernet 1/0
Device(CE1)(config-if)# ip rsvp source address 10.2.2.2
 <--------------------
Device(CE1)(config-if)# end
```

Configuring a Source Address on Device CE2 for the CE2-to-PE2 Interface

The following example configures a source address on the CE2-to-PE2 (Ethernet 0/0) interface in the figure above:

```
Device(CE2)# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Device(CE2)(config)# interface ethernet 0/0
Device(CE2)(config-if)# ip rsvp source address 10.6.6.6
 <--------------------
Device(CE2)(config-if)# end
```

Creating a Listener Proxy on Device C2

The following example creates a listener proxy on Device C2 and requests that the receiver reply with a RESV message for the flow if the PATH message destination is 10.7.7.7 in the figure above:

```
Device(C2)# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Device(C2)(config)# ip rsvp listener 10.7.7.7 any any reply <--------------------
Device(C2)(config)# end
```

Creating a Session from Device C1 to Device C2

The following example creates an RSVP session from Device C1 to Device C2:

```
Device(C1)# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(C1)(config)# ip rsvp sender-host 10.7.7.7 10.1.1.1 UDP 100 200 1 1 <-------------
Device(C1)(config)# end
```

Examples Verifying RSVP-Previous Hop Overwrite Configuration

Verifying the Source Address on Device CE1 for the CE1-to-PE1 Interface

The following example verifies the source address (10.2.2.2) configured on the CE1-to-PE1 (Ethernet 1/0) interface in the figure below:

```
Device(CE1)# show ip rsvp interface detail ethernet 1/0
 Et1/0:
   RSVP: Enabled
   Interface State: Up
   Bandwidth:
     Curr allocated: 1K bits/sec
     Max. allowed (total): 100K bits/sec
     Max. allowed (per flow): 100K bits/sec
     Max. allowed for LSP tunnels using sub-pools: 0 bits/sec
     Set aside by policy (total): 0 bits/sec
   Admission Control:
     Header Compression methods supported:
       rtp (36 bytes-saved), udp (20 bytes-saved)
   Traffic Control:
     RSVP Data Packet Classification is ON via CEF callbacks
   Signalling:
     DSCP value used in RSVP msgs: 0x3F
     Number of refresh intervals to enforce blockade state: 4
     Ip address used in RSVP objects: 10.2.2.2 <-----------------------------------
   Authentication: disabled
     Key chain:   <none>
     Type:        md5
     Window size: 1
     Challenge:   disabled
   Hello Extension:
     State: Disabled
```

Verifying the Source Address on Device CE2 for the CE2-to-PE2 Interface

The following example verifies the source address configured on the CE2-to-PE2 (Ethernet 0/0) interface in the figure below:

```
Device(CE2)# show ip rsvp interface detail ethernet 0/0
 Et0/0:
   RSVP: Enabled
   Interface State: Up
   Bandwidth:
     Curr allocated: 0 bits/sec
     Max. allowed (total): 100K bits/sec
     Max. allowed (per flow): 100K bits/sec
     Max. allowed for LSP tunnels using sub-pools: 0 bits/sec
     Set aside by policy (total): 0 bits/sec
   Admission Control:
     Header Compression methods supported:
       rtp (36 bytes-saved), udp (20 bytes-saved)
```

```
  Traffic Control:
    RSVP Data Packet Classification is ON via CEF callbacks
  Signalling:
    DSCP value used in RSVP msgs: 0x3F
    Number of refresh intervals to enforce blockade state: 4
    Ip address used in RSVP objects: 10.6.6.6 <----------------------------------
  Authentication: disabled
    Key chain:   <none>
    Type:        md5
    Window size: 1
    Challenge:   disabled
  Hello Extension:
    State: Disabled
```

Verifying the Listener Proxy on Device C2

The following example verifies the listener proxy configured on Device C2 in the figure below:

```
Device(C2)# show ip rsvp listeners
To               Protocol   DPort   Description                Action
10.7.7.7 <-------- any        any     RSVP Proxy                  reply
```

Verifying the Session from Device C1 to Device C2

The following example verifies that the session configured between Device C1 and Device C2 in the figure below is up:

```
Device(C1)# show ip rsvp reservation
To              From          Pro DPort Sport Next Hop      I/F      Fi Serv BPS
10.7.7.7       10.1.1.1       UDP 100   200   10.1.2.21     Et0/0    FF RATE 1K
```

Verifying the PHOP Address

The following example on Device CE2 verifies the source address configured on the CE1-to-PE1 interface in the figure below as the PHOP address:

```
Device(CE2)# show ip rsvp sender detail
PATH:
  Destination 10.7.7.7, Protocol_Id 17, Don't Police , DstPort 100
  Sender address: 10.1.1.1, port: 200
  Path refreshes:
    arriving: from PHOP 10.2.2.2 on Et0/0 every 30000 msecs <-------------------
  Traffic params - Rate: 1K bits/sec, Max. burst: 1K bytes
    Min Policed Unit: 0 bytes, Max Pkt Size 2147483647 bytes
  Path ID handle: CA000406.
  Incoming policy: Accepted. Policy source(s): Default
  Status:
  Output on Ethernet1/0. Policy status: Forwarding. Handle: 0E000402
    Policy source(s): Default
```

Verifying the Next-Hop Address

The following example on Device CE1 verifies the source address configured on the CE2-to-PE2 interface in the figure below as the next-hop address:

```
Device(CE1)# show ip rsvp reservation detail
RSVP Reservation. Destination is 10.7.7.7, Source is 10.1.1.1,
  Protocol is UDP, Destination port is 100, Source port is 200
  Next Hop: 10.6.6.6 on Ethernet1/0 <------------------------------------------
  Reservation Style is Fixed-Filter, QoS Service is Guaranteed-Rate
  Resv ID handle: 03000400.
  Created: 07:01:40 IST Tue Mar 25 2008
  Average Bitrate is 1K bits/sec, Maximum Burst is 1K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
```

```
Status:
Policy: Forwarding. Policy source(s): Default
```

Additional References

The following sections provide references related to the RSVP--Previous Hop Overwrite feature.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
QoS commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
QoS features including signaling, classification, and congestion management	"Quality of Service Overview" module

Standards

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

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2205	*Resource ReSerVation Protocol (RSVP)--Version 1 Functional Specification*
RFC 2209	*Resource ReSerVation Protocol (RSVP)--Version 1 Message Processing Rules*
RFC 3209	*RSVP-TE: Extensions to RSVP for LSP Tunnels*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for RSVP-Previous Hop Overwrite

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for RSVP--Previous Hop Overwrite

Feature Name	Releases	Feature Information
RSVP--Previous Hop Overwrite	12.4(20)T 15.0(1)SY	The RSVP--Previous Hop Overwrite feature allows you to configure a Resource Reservation Protocol (RSVP) device, on a per interface basis, to populate an address other than the native interface address in the previous hop (PHOP) address field of the PHOP object when forwarding a PATH message onto that interface. You can configure the actual address for the device to use, or an interface, including a loopback, from which to borrow the address. The following commands were introduced or modified: **debug ip rsvp, ip rsvp source, show ip rsvp interface.**

Glossary

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

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 that they want to receive.

RSVP Agent --Implements a Resource Reservation Protocol (RSVP) agent on Cisco IOS voice gateways that support Unified CM.

Unified Communcations Manager (CM)--The software-based, call-processing component of the Cisco IP telephony solution. The software extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications.