

RSVP MIB

Feature Summary

The Resource Reservation Protocol (RSVP) Management Information Base (MIB) feature introduces three new MIBs. The MIBs allow users to use SNMP to access objects belonging to RSVP, Integrated Services, and Guaranteed Services. The MIBs are defined according to RFCs 2206, 2213, and 2214, respectively. The RSVP MIB specifies two traps (NetFlow and LostFlow) which are triggered when a new flow is created or deleted.

Benefits

This feature allows a user on a remote management station to monitor RSVP-related information.

List of Terms

- **MIB**—Management Information Base. Database of network management information that is used and maintained by a network management protocol such as SNMP or CMIP. The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a GUI network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.
- **RSVP**—Resource Reservation Protocol. 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 forth) of the packet streams they want to receive. RSVP depends on IPv4. Also known as Resource Reservation Setup Protocol.
- **SNMP**—Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

Platforms

This feature is supported on the following platforms:

- Cisco 1600 series
- Cisco 2500 series
- Cisco 2600 series
- Cisco 3600 series

- Cisco 4000 series (Cisco 4000, 4000-M, 4500, 4500-M, 4700, 4700-M)
- Cisco 7200 series
- Cisco 7500/RSP series

Supported MIBs and RFCs

This feature supports the following MIBs:

- RSVP MIB
- Integrated Services MIB
- Integrated Services Guaranteed MIB

For descriptions of supported MIBs and how to use MIBs, see Cisco's MIB website on CCO at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

This feature supports the following RFCs:

- RFC 2206, *RSVP Management Information Base Using SMIPv2*
- RFC 2213, *Integrated Services Management Information Base Using SMIPv2*
- RFC 2214, *Integrated Services Management Information Base Guaranteed Service Extensions Using SMIPv2*

Configuration Task

With the exception of the RSVP MIB traps, no action is required to activate the MIBs. This MIB feature is automatically enabled when RSVP is turned on; however, RSVP traps must be enabled.

To enable RSVP traps, complete the following required configuration task:

- Enable RSVP Traps

Enable RSVP Traps

To enable RSVP traps, use the following command in global configuration mode:

Command	Purpose
<code>snmp-server enable traps rsvp</code>	Sends Resource Reservation Protocol (RSVP) notifications.

Configuration Example

The following example enables the router to send all RSVP traps to the host myhost.cisco.com using the community string public:

```
snmp-server enable traps rsvp
snmp-server host myhost.cisco.com public
```

Command Reference

This section documents new or modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command references.

- **snmp-server enable traps**

snmp-server enable traps

To enable the router to send SNMP traps and informs, use the **snmp-server enable traps** global configuration command. To disable SNMP notifications, use the **no** form of this command.

snmp-server enable traps [*notification-type*] [*notification-option*]
no snmp-server enable traps [*notification-type*] [*notification-option*]

Syntax Description

<i>notification-type</i>	<p>(Optional) Type of notification to enable. If no type is specified, all notifications are sent (including the envmon and repeater notifications). The notification type can be one of the following keywords:</p> <ul style="list-style-type: none"> • bgp—Sends Border Gateway Protocol (BGP) state change notifications. • config—Sends configuration notifications. • entity—Sends Entity MIB modification notifications. • envmon—Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded. When the envmon keyword is used, you can specify a <i>notification-option</i> value. • frame-relay—Sends Frame Relay notifications. • isdn—Sends Integrated Services Digital Network (ISDN) notifications. When the isdn keyword is used on Cisco 1600 series routers, you can specify a <i>notification-option</i> value. • repeater—Sends Ethernet hub repeater notifications. When the repeater keyword is selected, you can specify a <i>notification-option</i> value. • rsvp—Sends Resource Reservation Protocol (RSVP) notifications. • rtr—Sends response time reporter (RTR) notifications. • snmp—Sends Simple Network Management Protocol (SNMP) notifications. When the snmp keyword is used, you can specify a <i>notification-option</i> value. • syslog—Sends error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the logging history level command.
--------------------------	--

notification-option (Optional) When the **envmon** keyword is used, you can enable a specific environmental notification type, or accept all notification types from the environmental monitor system. If no option is specified, all environmental notifications are enabled. The option can be one or more of the following keywords: **voltage**, **shutdown**, **supply**, **fan**, and **temperature**.

When the **isdn** keyword is used, you can specify the **call-information** keyword to enable an SNMP ISDN call information notification for the ISDN MIB subsystem, or you can specify the **isdn-interface** keyword to enable an SNMP ISDN U interface notification for the ISDN U interface MIB subsystem.

When the **repeater** keyword is used, you can specify the repeater option. If no option is specified, all repeater notifications are enabled. The option can be one or more of the following keywords:

- **health**—Enables IETF Repeater Hub MIB (RFC 1516) health notification.
- **reset**—Enables IETF Repeater Hub MIB (RFC 1516) reset notification.

When the **snmp** keyword is used, you can specify the **authentication** option to enable SNMP Authentication Failure notifications. (The **snmp-server enable traps snmp authentication** command replaces the **snmp-server trap-authentication** command.) If no option is specified, all SNMP notifications are enabled.

Default

This command is disabled by default. Most notification types are disabled. However, some notification types cannot be controlled with this command. For example, some notification types are always enabled. Other notification types are enabled by a different command. For example, the linkUpDown notifications are controlled by the **snmp trap link-status** command.

If you enter this command with no *notification-type* keywords, the default is to enable all notification types controlled by this command.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1. The **rsvp** keyword was added in Cisco IOS Release 12.0(2)T.

This command is useful for disabling notifications that are generating a large amount of uninteresting or useless noise.

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types.

If you do not enter an **snmp-server enable traps** command, no notifications controlled by this command are sent. In order to configure the router to send these SNMP notifications, you must enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, all

notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled. In order to enable multiple types of notifications, you must issue a separate **snmp-server enable traps** command for each notification type and notification option.

The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.

For a host to receive a notification controlled by this command, both the **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled. If the notification type is not controlled by this command, just the appropriate **snmp-server host** command must be enabled.

The notification types used in this command all have an associated MIB object that allows them to be globally enabled or disabled. Not all of the notification types available in the **snmp-server host** command have notificationEnable MIB objects, so some of these cannot be controlled using the **snmp-server enable** command.

Examples

The following example enables the router to send all traps to the host myhost.cisco.com using the community string public:

```
snmp-server enable traps
snmp-server host myhost.cisco.com public
```

The following example enables the router to send Frame Relay and environmental monitor traps to the host myhost.cisco.com using the community string public:

```
snmp-server enable traps frame-relay
snmp-server enable traps envmon temperature
snmp-server host myhost.cisco.com public
```

The following example will not send traps to any host. The BGP traps are enabled for all hosts, but the only traps enabled to be sent to a host are ISDN traps.

```
snmp-server enable traps bgp
snmp-server host bob public isdn
```

The following example enables the router to send all inform requests to the host myhost.cisco.com using the community string public:

```
snmp-server enable traps
snmp-server host myhost.cisco.com informs version 2c public
```

The following example enables the router to send all RSVP traps to the host myhost.cisco.com using the community string public:

```
snmp-server enable traps rsvp
snmp-server host myhost.cisco.com public
```

Related Commands

snmp-server host
snmp-server informs
snmp-server trap-source
snmp trap illegal-address

