



SNMP Trap Support for the Virtual Switch Interface Master MIB

This feature module explains how to use the virtual switch interface (VSI) Master MIB to monitor and manage ATM switches that are connected to routers through the virtual switch interface.

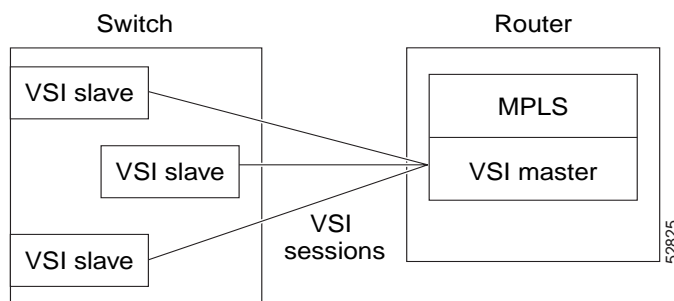
This document includes the following major sections:

- Feature Overview, page 1
- Supported Platforms, page 4
- Supported Standards, MIBs, and RFCs, page 4
- Prerequisites, page 4
- Configuration Tasks, page 5
- Command Reference, page 9
- Glossary, page 20

Feature Overview

The VSI master is a software module that resides on a router. The VSI master enables an application to control an ATM switch that is connected to the router. The VSI protocol runs between the VSI master and a VSI slave. The VSI master can communicate with more than one slave across a control interface that connects the router to the switch. Each master/slave connection is called a VSI session. Figure 1 illustrates VSI sessions between a VSI master and slaves.

Figure 1 VSI Master and VSI Slaves



Overview of the SNMP Trap Support for the VSI Master MIB

The VSI Master MIB allows you to manage and monitor the activities of the VSI components, including controllers, sessions, logical interfaces, and cross-connects. The MIB provides notifications in the form of traps when any of the VSI components change operational state, violate configured thresholds, or are added or removed.

The MIB allows you to specify which VSI components can send traps. To enable the traps for certain VSI components, you can use the MIB objects or Cisco IOS commands. See the section “Enabling Traps” for more information.

VSI Components You Can Monitor with the VSI Master MIB

The VSI Master MIB allows you to monitor the operation of the switch. It also displays the results of the operations. Specifically, the VSI Master MIB allows you to monitor:

- Connections between the router and the controlled switch.
- The status of the interfaces in the switch
- Virtual circuits (VCs) that are maintained across the interfaces.

MIB Traps

The VSI Master MIB allows you to enable traps on the following components:

Controllers—When VSI controllers are added or deleted

VSI sessions—When VSI sessions are established or disconnected

Logical interfaces—When logical interfaces become active or fail.

Cross-connects—When a cross-connect cannot be established.

Virtual circuits—When cross-connect resource thresholds are below configured thresholds.

MIB Objects

The following is a partial list of the supported MIB objects.

Controllers

You can obtain the following information about the controller:

- Controller identifier
- Number of cross-connects maintained in the switch
- Protocol version
- Controller interface index
- Slave interface identifiers
- Controller IP address

Sessions

You can obtain the following information about the VSI sessions:

- Virtual path identifiers (VPIs) for session connections
- Virtual circuit identifiers (VCIs) for the sessions
- Switch identifier
- Switch name
- Session state
- Protocol session monitoring

Logical Interfaces

Logical interfaces represent external interfaces that are available for connections. When you pair two external interfaces (represented by two logical interfaces), they provide a physical path through the switch. These physical paths support cross-connects. You can gather the following information about each logical interface:

- Interface name
- Operational state
- Administrative state
- Operational statistics
- Cross-connect usage
- Cross-connect availability
- Cross-connect capacity
- Interface capabilities
- VC ranges
- Interface index
- IP address

Cross-Connects

Cross-connects are virtual links across two interfaces. The participating interfaces that support these links are listed in the MIB's vsiLogicalIfTable entries. You can gather the following information about the cross-connects:

- Interface associations
- State
- Identifiers
- VPI/VCI identifiers for supporting interfaces

Restrictions

The VSI Master MIB is for ATM-LSRs running Multiprotocol Label Switching (MPLS).

Related Documents

See the following documents for more information:

- *Virtual Switch Interface Master MIB*

<http://www.cisco.com/public/mibs/v2/CISCO-VSIMASTER-MIB.my>

- *Multiprotocol Label Switching Overview*

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch_c/swprt3/xcftagov.htm

- *BPX Installation and Configuration Guide*, Chapter 23, “Configuring BXM Virtual Switch Interfaces”

http://www.cisco.com/univercd/cc/td/doc/product/wanbu/9_3/bpx/bpxi23.htm#xtocid120351

Supported Platforms

This feature is supported on the following routing platforms:

- Cisco 7200 series router
- Cisco MGX 8850 Route Processor Module (RPM)

You can use the following ATM switches to configure an ATM-LSR:

- Cisco BPX 8600, 8650, and 8680 switches
- MGX BXM cards

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

Virtual Switch Interface Master MIB

<http://www.cisco.com/public/mibs/v2/CISCO-VSIMASTER-MIB.my>

For descriptions of supported MIBs and how to use MIBs, see the Cisco MIB web site on Cisco Connection Online (CCO) at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

Memory Requirements

- The VSI Master MIB requires 75K of space.

- The runtime dynamic random-access memory (DRAM) is approximately 5K times the number of logical/slave interfaces the VSI controller manages.

Performance

The VSI cross-connect error messages can be invoked hundreds of times every second. To prevent a performance impact on the label switch controller (LSC), enable rate-limiting to control the amount of traffic that passes into or out of an interface.

Configuration Tasks

See the following sections for configuration tasks for the VSI Master MIB feature. Each task in the list indicates whether the task is optional or required.

- Enabling the SNMP Agent (required)
- Verifying That the SNMP Agent Has Been Enabled (optional)
- Enabling Traps (required)
- Setting Thresholds for Cross-Connects (optional)

Enabling the SNMP Agent

The SNMP agent for the VSI Master MIB is disabled by default. To enable the SNMP agent, perform the following steps:

	Command	Purpose
Step 1	prompt# telnet 10.10.10.1	Accesses the router through a Telnet session.
Step 2	router# enable	Enters the privileged mode.
Step 3	router# show running-configuration	Displays the running configuration to see if the SNMP agent is already running. If no SNMP information is present, continue with the steps below. If any SNMP commands are listed, you can modify them or leave them as they are.
Step 4	router# configure terminal	Enters the configuration mode.
Step 5	router(config)# snmp-server community xxxxxx RO	Enables the read-only community string, where xxxxxx is the read-only community string
Step 6	router(config)# exit	Exits the configuration mode and returns to the main prompt.
Step 7	router# write memory	Writes the modified configuration to nonvolatile memory (NVRAM) so that the settings stay permanently.

Verifying That the SNMP Agent Has Been Enabled

To verify that the SNMP agent has been enabled, perform the following steps:

- Step 1** Access the router through a Telnet session:
- ```
prompt# telnet 10.10.10.1
```
- Step 2** Enter the privileged mode:
- ```
router# enable
```
- Step 3** Display the running configuration and look for SNMP information:
- ```
router# show running-configuration
...
...
snmp-server community public RO
```

If you see any “snmp-server” statements, SNMP has been enabled on the router.

## Enabling Traps

SNMP notifications can be sent as traps or inform requests. A trap is an unsolicited message sent by an SNMP agent to an SNMP manager, indicating that some event has occurred. You can enable SNMP traps for the VSI Master MIB through the command line interface (CLI) or through an SNMP MIB object. The following sections explain these options.

### Using Commands to Enable the VSI Master MIB traps

To enable SNMP traps, use the **snmp-server enable traps** command. An SNMP agent can be configured to send traps when one of the VSI Master MIB objects changes. To enable VSI Master MIB traps to be sent from the agent to the manager, perform the following tasks in global configuration mode:

|        | Command                                                                 | Purpose                                          |
|--------|-------------------------------------------------------------------------|--------------------------------------------------|
| Step 1 | Router(config)# <b>snmp-server enable traps vsimaster</b>               | Enables the router to send VSI Master MIB traps. |
| Step 2 | Router(config)# <b>snmp-server host host community-string vsimaster</b> | Specifies the recipient of the trap message      |

Table 1 lists the CLI commands for enabling traps of specific VSI components.

**Table 1** CLI Commands that Control the Type of Traps You Receive

| To Receive Traps About              | Use This Command                                     |
|-------------------------------------|------------------------------------------------------|
| All components                      | <b>snmp server enable traps vsimaster</b>            |
| Controllers being added or deleted  | <b>snmp server enable traps vsimaster controller</b> |
| Sessions that connect or disconnect | <b>snmp server enable traps vsimaster session</b>    |

| To Receive Traps About                        | Use This Command                                            |
|-----------------------------------------------|-------------------------------------------------------------|
| Logical interfaces that connect or disconnect | <b>snmp server enable traps vsimaster logical-interface</b> |
| Cross-connects that fail                      | <b>snmp server enable traps vsimaster cross-connect</b>     |

## Using SNMP MIB Objects to Enable the VSI Master MIB Traps

You can also use MIB objects to specify which VSI components should send traps. To enable all VSI Master traps, use the vsiVSITrapEnable MIB object.

### Controller Traps

To enable traps about the status of the controller, use the vsiControllerTrapEnable MIB object. Table 2 lists the MIB objects that are specific to the controller.

**Table 2** *Controller Traps*

| To Receive Traps When   | Use This MIB Object  |
|-------------------------|----------------------|
| A controller is added   | vsiControllerAdded   |
| A controller is deleted | vsiControllerDeleted |

### VSI Session Traps

To enable traps about the status of the VSI sessions, use the vsiSessionTrapEnable MIB object. Table 3 lists the MIB objects that are specific to the VSI sessions.

**Table 3** *VSI Session Traps*

| To Receive Traps When         | Use This MIB Object |
|-------------------------------|---------------------|
| A VSI session is established  | vsiSessionUp        |
| A VSI session is disconnected | vsiSessionDown      |

### Logical Interfaces

To enable traps about the status of the logical interfaces, use the vsiLogicalIfTrapEnable MIB object. Table 4 lists the MIB objects that are specific to the logical interfaces.

**Table 4** *Logical Interface Traps*

| To Receive Traps When         | Use This MIB Object |
|-------------------------------|---------------------|
| A logical interface is active | vsiLogicalIfUp      |
| A logical interface fails     | vsiLogicalIfDown    |

### Cross-connects

To enable traps about the status of the cross-connects, use the vsiXCTrapEnable MIB object. Table 5 lists the MIB objects that are specific to the cross-connects.

**Table 5** *Cross-connect Traps*

| To Receive Traps When                                         | Use This MIB Object    |
|---------------------------------------------------------------|------------------------|
| A cross-connect cannot be established                         | vsiXCFailed            |
| The LCN resources drop, possibly causing resource exhaustion. | vsiLcnExhaustionNotice |

## Setting Thresholds for Cross-Connects

When cross-connects on XtagATM interfaces are created or deleted, a counter keeps a tally of the available logical channel number (LCN) resources. If the LCN resources become too low, the MIB sends messages to alert you of the possibility of resource exhaustion.

You must first set the warning and alarm thresholds for the number of LCNs. To set the warning threshold, use the `vsiAvailableChnlWarnThreshold` MIB object. To set the alarm threshold, use the `vsiAvailableChnlAlarmThreshold` MIB object. The following list explains the usage guidelines of these MIB objects:

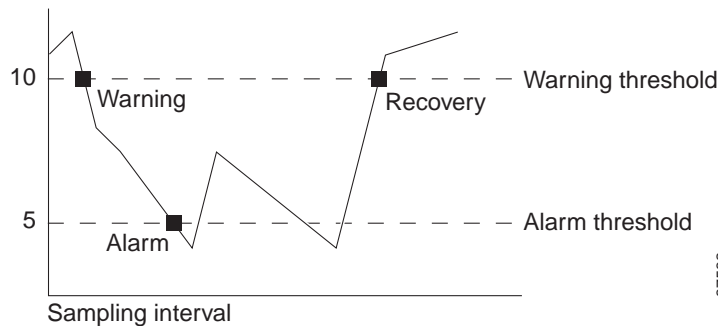
- The threshold range is 1 to 100.
- The warning threshold value must be greater than or equal to the value of the alarm threshold. Likewise, the alarm threshold value must be less than or equal to the value of the warning threshold.
- If you only set one threshold, the MIB automatically sets the other threshold value to the same value as the threshold value you set.
- By default, the threshold functionality is disabled.

The following list explains the conditions under which warnings, alarms, and other messages are sent. Figure 2 illustrates the thresholds.

- If the number of LCNs falls below the the warning threshold, a warning is sent. This message indicates that the potential for resource exhaustion is possible.
- If the number of LCNs falls below the alarm threshold, an alarm is generated. This message indicates that the potential for resource exhaustion is imminent. If resource exhaustion occurs, cross-connects cannot be set up.
- If the number of LCNs returns to above the warning threshold, a recovery message is generated. This message means that the potential for resource exhaustion no longer exists.
- If the number of LCNs never crosses any threshold during the polling period, a normal message is generated.

To prevent an overwhelming number of warnings or alarms from being generated during a sampling period, only one warning or alarm is generated when the number of LCNs falls below the threshold. The number of LCNs must return to normal before another warning or alarm is generated.

Figure 2 Warning and Alarm Thresholds

**Note**

If XtagATM interfaces share resources, the LCN does not represent the actual amount of available resources. For example, the interfaces XtagATM1 and XtagATM2 share resources. If a cross-connect is set up on XtagATM1 but not on XtagATM2, XtagATM1 takes resources away from XtagATM2. When the VSI slave reports the available resources, it only reports on the resources for XtagATM1. The resources for XtagATM2 are not reported. This is because the VSI slave provides updates only when a cross-connect is set up or torn down or when the slave's resources are partitioned. Any interfaces that are not set up or torn down do not send updates. As a result, if XtagATM2 doesn't have enough resources in the resource pool, the problem does not get reported.

## Configuration Examples

In the following example, the SNMP agent is enabled.

```
snmp-server community
```

In the following example, SNMPv1 and SNMPv2C are enabled. The configuration permits any SNMP manager to access all objects with read-only permissions using the community string *public*.

```
snmp-server community public
```

In the following example, read-only access is granted for all objects to members of access list 4 that specify the *comaccess* community string. No other SNMP managers have access to any objects.

```
snmp-server community comaccess ro 4
```

In the following example VSI Master MIB traps are sent to the host *cisco.com*. The community string is restricted. The first line enables the router to send VSI Master MIB traps in addition to any traps previously enabled. The second line specifies the destination of these traps and overwrites any previous **snmp-server host** commands for the host *cisco.com*.

```
snmp-server enable traps vsi master
snmp-server host cisco.com restricted vsimaster
```

## Command Reference

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

## snmp-server community

Use the **snmp-server community** global configuration command to configure read-only or read-write Simple Network Management Protocol (SNMP) community strings. Use the **no snmp-server community** command to change the community string to its default value.

**snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [*number*]

**no snmp-server community** *string*

### Syntax Description

|                              |                                                                                                                                                                                |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>string</i>                | Community string of 1 to 32 alphanumeric characters. The community string acts like a password and permits access to the SNMP protocol. No blank character spaces are allowed. |
| <b>view</b> <i>view-name</i> | (Optional) Name of a previously defined view. The view defines the objects available to the community.                                                                         |
| <b>ro</b>                    | (Optional) Configures read-only access. Authorized management stations can only retrieve MIB objects.                                                                          |
| <b>rw</b>                    | (Optional) Configures read-write access. Authorized management stations can retrieve and modify MIB objects.                                                                   |
| <i>number</i>                | (Optional) Integer from 1 to 99 that specifies an access list of IP addresses that are allowed to use the community string to gain access to the SNMPv1 agent.                 |

### Defaults

Read-only (**ro**)

The default value of the read-only community string is public, and the default value of the read-write community string is private.

### Command Modes

Global configuration

### Command History

| Release                | Modification                 |
|------------------------|------------------------------|
| Cisco IOS Release 10.0 | This command was introduced. |

### Usage Guidelines

The **no snmp-server** command disables both versions of SNMP (SNMPv1 and SNMPv2). The first **snmp-server** command that you enter enables both versions of SNMP.

### Examples

In this example, the read-write community string is set to *newstring*:

```
hostname (config)# snmp-server community newstring rw
```

In the following example, the string *comaccess* is assigned to SNMPv1 allowing read-only access. IP access list 4 can use the community string:

```
snmp-server community comaccess ro 4
```

In the following example, the string *mgr* is assigned to SNMPv1, allowing read-write access to the objects in the restricted view:

```
snmp-server community mgr view restricted rw
```

The following command removes the community *comaccess*:

```
no snmp-server community comaccess
```

The following command disables both versions of SNMP:

```
no snmp-server
```

---

**Related Commands**

| Command                         | Description                                        |
|---------------------------------|----------------------------------------------------|
| <b>snmp-server host</b>         | Specifies the recipient of an SNMP trap operation. |
| <b>snmp-server enable-traps</b> | Enables the router to send SNMP traps.             |

## snmp-server enable traps

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

**snmp-server enable traps** [*notification-type*] [*notification-option*]

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

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syntax Description</b> | <i>notification-type</i> (Optional) Type of notification to enable. If no type is specified, all notifications are sent (including the envmon and repeater notifications).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>keywords</b>           | <p>The <i>notification-type</i> can use one of the following strings:</p> <p><b>bgp</b>—Sends Border Gateway Protocol (BGP) state change notifications.</p> <p><b>config</b>—Sends configuration notifications.</p> <p><b>entity</b>—Sends entity MIB modification notifications.</p> <p><b>envmon</b>—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.</p> <p><b>frame-relay</b>—Sends Frame Relay notifications.</p> <p><b>hsrp</b>—Sends Hot Standby Routing Protocol (HSRP) notifications.</p> <p><b>isdn</b>—Sends Integrated Services Digital Network (ISDN) notifications.</p> <p><b>repeater</b>—Sends Ethernet hub repeater notifications. When the repeater keyword is selected, you can specify a <i>notification-option</i> value.</p> <p><b>vsimaster</b>—Sends VSI master notifications. When the vsimaster keyword is selected, you can specify a <i>notification-option</i> value.</p> <p><b>rtr</b>—Sends response time reporter (RTR) notifications.</p> <p><b>snmp</b>—Sends SNMP notifications. When you use the snmp keyword, you can specify a <i>notification-option</i> value.</p> <p><b>syslog</b>—Sends error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the logging history level command.</p> |

---

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>notification-option</i> | (Optional) Type of notification option to enable.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>keywords</b>            | <p>The <i>notification-option</i> keyword can use any of the following keywords:</p> <p><b>envmon</b>—When the <b>envmon</b> 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 types are enabled. The notification option can be one or more of the following keywords:</p> <ul style="list-style-type: none"> <li><b>fan</b></li> <li><b>shutdown</b></li> <li><b>supply</b></li> <li><b>temperature</b></li> <li><b>voltage</b></li> </ul> <p><b>repeater</b>—When the <b>repeater</b> keyword is used, you can specify any of the following options. If no option is specified, all repeater types are enabled. The option can be one or more of the following keywords:</p> <ul style="list-style-type: none"> <li><b>health</b>—Enables Internet Engineering Task Force (IETF) Repeater Hub MIB (RFC 1516) health notification.</li> <li><b>reset</b>—Enables the IETF Repeater Hub MIB (RFC 1516) reset notification.</li> </ul> <p><b>isdn</b>—When the <b>isdn</b> keyword is used, you can specify one of the following keywords:</p> <ul style="list-style-type: none"> <li><b>call-information</b>—Enables an SNMP ISDN call information notification for the ISDN MIB subsystem.</li> <li><b>isdn-interface</b>—Enables an SNMP ISDN U interface notification for the ISDN U interface MIB subsystem.</li> </ul> <p><b>snmp</b>—When the <b>snmp</b> keyword is used, you can specify the following keywords. If no option is specified, all SNMP notifications are enabled.</p> <ul style="list-style-type: none"> <li><b>authentication</b>—Enables SNMP Authentication Failure notifications. (The command <b>snmp-server enable traps snmp authentication</b> replaces the <b>snmp-server trap-authentication</b> command.)</li> </ul> <p><b>vsimaster</b>—When the <b>vsimaster</b> keyword is used, you can specify any of the following keywords. If no option is specified, all vsi master traps types are enabled. The option can be one or more of the following keywords:</p> <ul style="list-style-type: none"> <li><b>controller</b></li> <li><b>session</b></li> <li><b>logical interface</b></li> <li><b>cross-connect</b></li> </ul> |

---



---

## Defaults

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 History**

| Release                    | Modification                            |
|----------------------------|-----------------------------------------|
| Cisco IOS Release 11.1     | This command first appeared.            |
| Cisco IOS Release 12.2(2)T | The <b>vsimaster</b> keyword was added. |

**Usage Guidelines**

Issue the **snmp-server enable traps** command to specify which SNMP traps the router sends, and issue the **snmp-server host** command to specify which host or hosts receive SNMP traps.

You must issue a separate **snmp-server enable traps** command for each trap type.

This command is useful for disabling notifications that generate a large amount of 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. 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. 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 with the **snmp-server host** command. Issue the **snmp-server host** command to specify which host or hosts receive SNMP notifications. 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 associated MIB objects 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 notifications cannot be controlled with the **snmp-server enable** command.

**Examples**

The following commands enable the router to send Frame Relay and environmental monitor traps:

```
snmp-server enable traps frame-relay
snmp-server enable traps envmon temperature
```

The following commands enable 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 commands enable 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
```

| Related Commands | Command                        | Description                                                                                                |
|------------------|--------------------------------|------------------------------------------------------------------------------------------------------------|
|                  | <b>snmp-server host</b>        | Specifies the recipient of an SNMP notification operation,                                                 |
|                  | <b>snmp-server trap-source</b> | Specifies the interface (and hence the corresponding IP address) from which an SNMP trap should originate. |

## snmp-server host

To specify the recipient of an SNMP notification operation, issue the **snmp-server host** global configuration command. The **no** form of this command prevents the specified host from receiving SNMP notifications. You must configure at least one host to receive notifications.

```
snmp-server host host [traps | informs] version { 1 | 2c | 3 [{ auth | priv }]} community-string
[udp-port port] [notification-type]
```

```
no snmp-server host host community-string [traps | informs]
```

### Syntax Description

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>host</i>                 | Name or Internet address of the host.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>traps</b>                | (Optional) Send SNMP traps to the host. This is the default.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>informs</b>              | (Optional) Send SNMP informs to the host.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>version</b>              | (Optional) Specify the version of SNMP used to send the traps.<br><b>1</b> = SNMPv1 (This option is the default and is not available with the informs option.)<br><b>2c</b> = SNMPv2C<br><b>3</b> = SNMPv3 You can specify either of the following: <ul style="list-style-type: none"> <li>– <b>auth</b>—(Optional) Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication.</li> <li>– <b>priv</b>—(Optional) Enables Data Encryption Standard (DEC) packet encryption (also called privacy).</li> </ul> <b>Note:</b> If you specify SNMPv3 without the <b>auth</b> or <b>priv</b> keyword, the level of security is noAuthPriv. |
| <i>community-string</i>     | Password-like community string sent with the notification operation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>udp-port</b> <i>port</i> | User Datagram Protocol (UDP) port of the host. The default is 162.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>notification-type</i> | (Optional) Type of notification to be sent to the host. If no type is specified, all notifications are sent.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>keywords</b>          | <p>The notification type can be one or more of the following keywords:</p> <p><b>bgp</b>—Sends Border Gateway Protocol (BGP) state change notifications.</p> <p><b>config</b>—Sends configuration notifications.</p> <p><b>dspu</b>—Sends downstream physical unit (DSPU) notifications.</p> <p><b>entity</b>—Sends Entity MIB modification notifications.</p> <p><b>envmon</b>—Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded.</p> <p><b>frame-relay</b>—Sends Frame Relay notifications.</p> <p><b>hsrp</b>—Sends Hot Standby Routing Protocol (HSRP) notifications</p> <p><b>isdn</b>—Sends Integrated Services Digital Network (ISDN) notifications.</p> <p><b>llc2</b>—Sends Logical Link Control, type 2 (LLC2) notifications.</p> <p><b>vsimaster</b>—Sends VSI Master notifications.</p> <p><b>rptr</b>—Sends standard repeater (hub) notifications.</p> <p><b>rsrb</b>—Sends remote source-route bridging (RSRB) notifications.</p> <p><b>rtr</b>—Sends response time reporter (RTR) notifications.</p> <p><b>sdlc</b>—Sends Synchronous Data Link Control (SDLC) notifications.</p> <p><b>sdllc</b>—Sends SDLLC notifications.</p> <p><b>snmp</b>—Sends Simple Network Management Protocol (SNMP) notifications defined in RFC 1157.</p> <p><b>stun</b>—Sends serial tunnel (STUN) notifications.</p> <p><b>syslog</b>—Sends error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the logging history level command.</p> <p><b>tty</b>—Sends Cisco enterprise-specific notifications when a Transmission Control Protocol (TCP) connection closes.</p> <p><b>x25</b>—Sends X.25 event notifications.</p> |

### Defaults

This command is disabled by default. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types.

If you do not specify the **version**, the default is version 1.

If you do not specify **traps** or **informs**, traps are enabled.

The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, issue the **no snmp-server host informs** command.

### Command Modes

Global configuration

**Command History**

| Release                    | Modification                            |
|----------------------------|-----------------------------------------|
| Cisco IOS Release 10.0.    | This command was introduced.            |
| Cisco IOS Release 12.2(2)T | The <b>vsimaster</b> keyword was added. |

**Usage Guidelines**

When multiple **snmp-server host** commands specify the same host, the community string in the last command is used, and the notification types set in the last command filter the SNMP messages sent to that host.

To control which traps are sent by the router, issue the **snmp-server enable traps** command.

Whether a notification-type option is available or not depends on the router type and the Cisco IOS software features supported on the router. For example, the **envmon** keyword is available only if the environmental monitor is part of the system.

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once, but an inform can be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications controlled by this command are sent. To configure the router to send those SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host. To enable multiple hosts, you must issue a separate **snmp-server host** command for each host.

You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command remains in effect. For example, if you enter an **snmp-server host** inform command for a host and then enter another **snmp-server host** inform command for the same host, the second command replaces the first.

The **snmp-server host** command is used with the **snmp-server enable** command. Issue the **snmp-server enable** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable** command and the **snmp-server host** command for that host must be enabled.

However, some notification types cannot be controlled with the **snmp-server enable** 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. These notification types do not require an **snmp-server enable** command.

**Examples**

The following command sends the SNMP traps defined in RFC 1157 to the host cisco.com. The community string is comaccess.

```
snmp-server host cisco.com comaccess snmp
```

The following command sends the SNMP and Cisco environmental monitor enterprise-specific traps to address 172.30.2.160:

```
snmp-server host 172.30.2.160 snmp envmon
```

**Related Commands**

| Command                         | Description                                                                                                |
|---------------------------------|------------------------------------------------------------------------------------------------------------|
| <b>snmp-server enable traps</b> | Enables the router to send SNMP traps and informs.                                                         |
| <b>snmp-server trap-source</b>  | Specifies the interface (and hence the corresponding IP address) from which an SNMP trap should originate. |
| <b>snmp-server trap-timeout</b> | Specifies how often to send trap messages.                                                                 |

# Glossary

**agent**—A process in the device that handles SNMP requests.

**alarm**—A message that is triggered when defined values cross a given threshold. For instance, you can specify the number of Ethernet collisions, plus a time interval, such as 1 second, and a threshold, such as 60 collisions. Given this scenario, an alarm is generated when the number of Ethernet collisions exceeds 60 in 1 second.

**event**—The action that is triggered as result of an alarm. Alarms and events are logically connected. For example, when the number of collisions on an Ethernet segment exceeds 60 per second, the corresponding event can cause a trap message to be sent to one or more management stations.

An event is generated by the RMON agent, which could be triggered by a threshold crossing. An event can be signaled as a trap, a new entry in the MIB log table, both, or neither.

**inform request**—A message sent by an SNMP agent to a network management station, console, or terminal to indicate that a significant event occurred. SNMP inform requests are more reliable than traps because an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the manager does not receive an inform request, it does not send a response. If the sender never receives a response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.

**Management Information Base**—See MIB.

**MIB**—Management Information Base. Database of network management information that is used and maintained by a network management protocol such as SNMP. The value of a MIB object can be changed or retrieved by SNMP commands, usually through a network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

**MPLS**—Multiprotocol label switching. MPLS is a method for forwarding packets (frames) through a network. It enables routers at the edge of a network to apply labels to packets (frames). ATM switches or existing routers in the network core can switch packets according to the labels.

**Multiprotocol Label switching**—See MPLS.

**Simple Network Management Protocol**—See SNMP.

**SNMP**—Simple Network Management Protocol. 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.

**threshold**—The range in which you expect your network to perform. If a performance exceeds or goes below the expected bounds, you can examine these areas for potential problems. You can create thresholds for a specific device.

**trap**—Message sent by an SNMP agent to a network management station, console, or terminal to indicate that a significant event occurred. Traps are less reliable than inform requests, because the receiver does not send an acknowledgment when it receives a trap. The sender cannot determine if the trap was received.

**VSI**—Virtual Switch Interface. A proposed common control interface to Cisco switches. The VSI can manage connections and discover configuration information about the switch.

**VSI controller**—A controller, such as a PNNI SVC controller, Portable AutoRoute or MPLS controller, that controls a switch using the VSI.

**VSI master**—A V process implementing the master side of the VSI protocol in a VSI controller. Sometimes the whole VSI controller might be referred to as a “VSI Master,” but this is not strictly correct. Also, the VSI master is a device that controls a VSI switch, for example, a VSI Label Switch Controller.

**VSI slave**—A VSI slave is either of the following:

1. A switch (when one router controls one slave) or a port card (when one router controls more than one slave) that implements the VSI.
2. A process implementing the slave side of the VSI protocol.

