SNMP Trap Support for the Virtual Switch Interface Master MIB

Last Updated: December 4, 2012

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.

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 SNMP Trap Support for the VSI Master MIB

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.

Restrictions for SNMP Trap Support for the VSI Master MIB

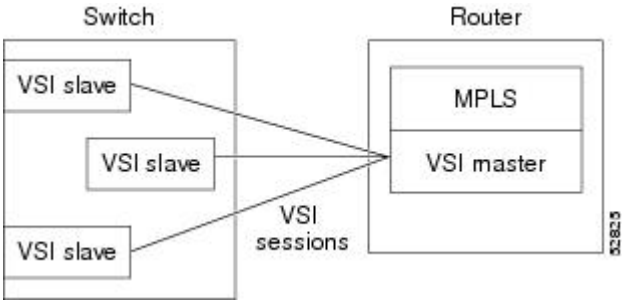
The VSI Master MIB is for ATM-LSRs running Multiprotocol Label Switching (MPLS).

Information About SNMP Trap Support for the VSI Master MIB

VSI Master and Slave

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. The figure below illustrates VSI sessions between a VSI master and slaves.

Figure 1 VSI Master and VSI Slaves



VSI Components That 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

How to Configure SNMP Trap Support for the VSI Master MIB

Enabling the SNMP Agent

The SNMP agent for the VSI Master MIB is disabled by default. To enable the SNMP agent, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **show running-configuration**
3. **configure terminal**
4. snmp-server community *string* RO
5. **exit**
6. write memory

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show running-configuration** **Example:** `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 3	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 4	snmp-server community *string* RO **Example:** `router(config)# snmp-server community` *string* `RO`	Enables the read-only community string, where *string* is the read-only community string.
Step 5	**exit** **Example:** `router(config)# exit`	Exits the configuration mode and returns to the main prompt.
Step 6	write memory **Example:** `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 steps in this section.

SUMMARY STEPS

1. **enable**
2. **show running-configuration**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show running-configuration** **Example:** `Router# show running-configuration`	Displays the running configuration to see if the SNMP agent is already running. 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.

- Enabling the VSI Master MIB Traps by Using Commands, page 6
- Enabling the VSI Master MIB Traps by Using SNMP MIB Objects, page 7

Enabling the VSI Master MIB Traps by Using Commands

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.

The table below 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	**snmp server enable traps vsimaster**
Controllers being added or deleted	**snmp server enable traps vsimaster controller**
Sessions that connect or disconnect	**snmp server enable traps vsimaster session**
Logical interfaces that connect or disconnect	**snmp server enable traps vsimaster logical-interface**
Cross-connects that fail	**snmp server enable traps vsimaster cross-connect**

To enable VSI Master MIB traps to be sent from the agent to the manager, perform the following tasks in global configuration mode:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps vsimaster**
4. **snmp-server host** *hostname community-string* **vsimaster**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps vsimaster** **Example:** `router(config)# snmp-server enable traps vsimaster`	Enables the router to send VSI Master MIB traps.
Step 4	**snmp-server host** *hostname community-string* **vsimaster** **Example:** `router(config)# snmp-server host cisco.com restricted vsimaster`	Specifies the recipient of the trap message
Step 5	**exit** **Example:** `router(config)# exit`	Exits the configuration mode and returns to the main prompt.

Enabling the VSI Master MIB Traps by Using SNMP MIB Objects

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. The table below 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. The table below 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. The table below 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. The table below 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:

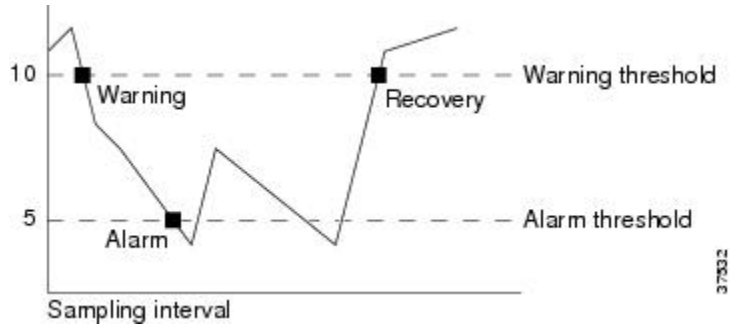
- The threshold range is 1 to 100.
- The warning threshold value must be greater than or equal to the value of the alarm threshold. Likewise, the alarm threshold value must be less than or equal to the value of the warning threshold.
- If you only set one threshold, the MIB automatically sets the other 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. The figure below 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 for SNMP Trap Support for the VSI Master MIB

Enabling the SNMP Agent Example

In the following example, the SNMP agent is enabled.

```
snmp-server community
```

Enabling the SNMP Agent with a Community String Example

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
```

Enabling the SNMP Agent with Read-Only Access to Access List Members Example

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

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

Enabling Traps and Specifying the Trap Recipient Example

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 vsimaster
snmp-server host cisco.com restricted vsimaster
```

Additional References

Related Documents

Related Topic	Document Title
ATM commands	*Cisco IOS Asynchronous Transfer Mode Command Reference*
MPLS concepts	"Multiprotocol Label Switching Overview" chapter of the *Cisco IOS Multiprotocol Label Switching Configuration Guide*, Release 12.4T

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
CISCO-VSIMASTER-MIB	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
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for SNMP Trap Support for the VSI Master MIB

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 6 Feature Information for SNMP Trap Support for the Virtual Switch Interface Master MIB

Feature Name	Releases	Feature Information
SNMP Trap Support for the Virtual Switch Interface Master MIB	12.2(2)T, 12.4(20)T	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. The following commands were introduced or modified: **snmp-server community**, **snmp-server enable traps**, **snmp-server host**. Support was removed for this feature in Cisco IOS Release 12.4(20)T and later releases.

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 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.