



ATM PVC Trap Support

Feature Summary

The ATM PVC Trap Support feature allows you to use SNMP to provide ATM PVC failure notification and access to PVC status tables.

PVC Failure Notification

This feature provides ATM PVC failure notification by sending a trap when a PVC on an ATM interface fails or leaves the UP operational state.

Only one trap is generated per hardware interface, within the specified interval defined by `atmIntPvcNotificationInterval`. If other PVCs on the same interface go DOWN during this interval, traps are generated and held until the interval has elapsed. Once the interval has elapsed, the traps are sent if the PVCs are still DOWN.

No trap is generated when a PVC returns to the UP state after having been in the DOWN state. If you need to detect the recovery of PVCs, you must use the SNMP management application to regularly poll your router.

PVC Status Tables

When ATM PVC Trap Support is enabled, the SNMP manager can poll the SNMP agent to get PVC status information. This feature supports the table `atmInterfaceExtTable` which provides PVC status on an ATM interface. It also supports the table `atmCurrentlyFailingPvcTable` which provides currently failing and previously failed PVC time-stamp information.

Benefits

Normally, an SNMP manager is not notified when an ATM PVC goes DOWN. With ATM PVC Trap Support enabled, an SNMP agent can notify the SNMP manager when a PVC goes DOWN by sending the required PVC traps.

List of Terms

Asynchronous Transfer Mode (ATM)—International standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length (53-byte) cells. Fixed-length cells allow cell processing to occur in hardware, thereby reducing transit delays. ATM is designed to take advantage of high-speed transmission media such as E3, SONET, and T3.

Management Information Base (MIB)—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.

Network Management System (NMS)—System responsible for managing at least part of a network. An NMS is generally a reasonably powerful and well-equipped computer such as an engineering workstation. NMSs communicate with agents to help keep track of network statistics and resources.

Operation, Administration, and Maintenance (OAM)—ATM Forum specifies OAM cells used to monitor virtual circuits. OAM cells provide a virtual circuit-level loopback in which a router responds to the cells, demonstrating that the circuit is up, and the router is operational.

permanent virtual circuit (PVC)—Virtual circuit that is permanently established. PVCs save bandwidth associated with circuit establishment and tear down in situations where certain virtual circuits must exist all the time. In ATM terminology, PVC also stands for permanent virtual connection.

permanent virtual circuit link (PVCL)—Refers to the local link between a host and a switch or between switches.

permanent virtual path link (PVPL)—Refers to a group of local links between a host and a switch or between switches.

Simple Network Management Protocol (SNMP)—An application-layer protocol that provides a message format for communication between SNMP managers and agents and is 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.

SNMP agent—Resides on the router and contains MIB variables whose values the SNMP manager can request or change. The agent gathers information from the MIB, responds to a manager's requests to get or set data, and sends unsolicited traps to the manager.

SNMP manager—Can be part of an NMS such as CiscoWorks. The manager can get a MIB value from an agent or store a MIB value into that agent.

trap—A message from an SNMP agent alerting the SNMP manager to a condition on the network.

Restrictions

This feature supports only permanent virtual circuit links (PVCLs), not permanent virtual path links (PVPLs).

Platforms

This feature is supported on all ATM interfaces on these platforms:

- Cisco 4500
- Cisco 4700
- Cisco 7200 series
- Cisco 7500 series
- Cisco 12000 series

Prerequisites

Before you enable this feature, you must configure SNMP support and an IP routing protocol on your router. See the “Configuration Example” section later in this document. For more information about configuring SNMP support, refer to the chapter “Monitoring the Router and Network” in the *Configuration Fundamentals Configuration Guide* for Cisco IOS Release 12.0. For information about configuring IP routing protocols, refer to the section “IP Routing Protocols” in the *Network Protocols Configuration Guide, Part 1* for Cisco IOS Release 12.0.

To receive PVC failure notification and access to PVC status tables on your router, you must have the Cisco ATM PVC trap MIB called CISCO-IETF-ATM2-PVCTRAP-MIB.my compiled in your NMS application. You can find this MIB on the Web at Cisco’s MIB website that has the URL <http://www.cisco.com/public/mibs>.

Supported MIBs and RFCs

The ATM PVC Trap Support feature contains the following two tables and one trap:

- The table atmInterfaceExtTable displays PVC status on an ATM interface and is indexed by ifIndex. This table contains the following objects:
 - atmIntfPvcFailures
 - atmIntfCurrentlyFailingPVcls
 - atmIntfPvcFailuresTrapEnable
 - atmIntfPvcNotificationInterval
 - atmPreviouslyFailedPVclInterval
- The table atmCurrentlyFailingPVclTable displays time-stamp information for currently failing and previously failed PVCs and is indexed by ifIndex, atmVclVpi, and atmVclVci. This table contains the following objects:
 - atmCurrentlyFailingPVclTimeStamp
 - atmPreviouslyFailedPVclTimeStamp
- The PVC trap atmIntPvcFailuresTrap contains the following objects:
 - ifIndex
 - atmIntfPvcFailures
 - atmIntfCurrentlyFailingPVcls

The new objects in this feature are defined in the IETF draft *The Definitions of Supplemental Managed Objects for ATM Management*, which is an extension to the *AToM MIB* (RFC 1695). You can find this draft on the Web at the following URL: <http://www.ietf.org/internet-drafts/>.

Note *The Interfaces Group MIB using SMIPv2* (RFC 2233) is now available for ATM subinterfaces if you are running Cisco IOS Release 12.0(1)T or later. If you want this capability, you must add the new ifType called atmSubInterface (IANA ifType number = 134) to the Interfaces Group MIB and compile it in your NMS application. You can get this new ifType in the file called IANAifType-MIB.my on the Web at Cisco’s MIB website with URL <http://www.cisco.com/public/mibs>. This capability is supported on Cisco 4500, Cisco 4700, Cisco 7200 series, Cisco 7500 series, and Cisco 12000 series routers.

Configuration Task

When you configure ATM PVC Trap Support, you must also enable OAM management on the PVC. To enable ATM PVC Trap Support and OAM management, use the following commands beginning in global configuration mode:

Step	Command	Purpose
1	snmp-server enable traps atm pvc interval <i>seconds</i> fail-interval <i>seconds</i>	Enable the ATM PVC Trap Support feature.
2	interface atm slot/0[.subinterface-number{ multipoint point-to-point}] or interface atm slot/port-adapter/0[.subinterface-number{ multipoint point-to-point}] or interface atm number[.subinterface-number{ multipoint point-to-point}]	Specify the ATM interface using the appropriate form of the interface atm command. ¹
3	pvc [name] vpi/vci	Enable the PVC.
4	oam-pvc manage	Enable end-to-end OAM management for an ATM PVC.

1 Use the **interface atm slot/0** command with the AIP on Cisco 7500 series routers or any ATM port adapter on the Cisco 7200 series routers. Use the **interface atm slot/port-adapter/0** command with any ATM port adapter on the Cisco 7500 series routers. Use the **interface atm number** command with the NPM on the Cisco 4500 and 4700 routers.

For more information on OAM management, see the section “Configure VC Management” in the “Configuring ATM” chapter of the *Wide-Area Networking Configuration Guide* for Cisco IOS Release 12.0.

Configuration Example

The following example configures the ATM PVC Trap Support feature on your Cisco router:

```
!For ATM PVC Trap Support to work on your router, you must first have SNMP support and
!an IP routing protocol configured on your router:
Router(config)# snmp-server community public ro
Router(config)# snmp-server host 171.69.61.90 public
```

```
Router(config)# ip routing
Router(config)# router igrp 109
Router(config-router)# network 172.21.0.0
!
!Enable ATM PVC Trap Support and OAM management:
Router(config)# snmp-server enable traps atm pvc interval 40 fail-interval 10
Router(config)# interface atm 1/0.1
Router(config-if)# pvc 0/1
Router(config-if-atm-vc)# oam-pvc manage
!
! Now if PVC 0/1 goes down, host 171.69.61.90 will receive traps.
```

Command Reference

This section documents additions to the **snmp-server enable traps** command for the ATM PVC Trap Support feature. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command references.

snmp-server enable traps

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

```
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"> • atm—Enables the ATM PVC Trap Support feature. • 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 used, you can specify a <i>notification-option</i> value. • 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 either 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 **isdnu-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.

When the **atm** keyword is used, specify the interval between traps as follows:

- **pvc interval** *seconds*—Minimum period between successive traps, in the range 1 to 3600.
- **pvc fail-interval** *seconds*—Minimum period for storing the failed time-stamp, in the range 0 to 3600.

Defaults

This command is disabled by default. Most notification types are disabled. However, some notification types cannot be controlled with this command, because they 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. Cisco IOS Release 12.0(1)T introduced the flag to enable ATM PVC traps.

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, notifications controlled by this command are not 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 atm pvc** command enables the ATM PVC Trap Support feature and requires trap intervals (**interval seconds** and **fail-interval seconds**) to be set.

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 objects cannot be controlled using the **snmp-server enable** command.

Examples

The following example enables ATM PVC Trap Support on ATM interface 1/0.1:

```
snmp enable traps atm pvc interval 40 fail-interval 10
interface atm 1/0.1
pvc 0/1
oam-pvc manage
```

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 does 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
```

Related Commands

- interface atm**
- oam-pvc manage**
- pvc**
- snmp-server host**
- snmp-server informs**
- snmp-server trap-source**
- snmp trap illegal-address**

