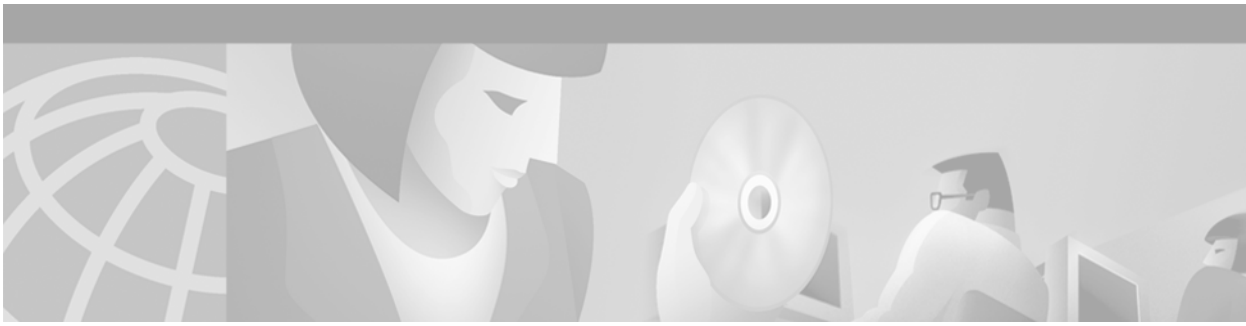

MSDP MIB

This feature module describes the Multicast Source Discovery Protocol (MSDP) Management Information Base (MIB) support added for SNMP network monitoring in Cisco IOS Release 12.0(12)S. It includes information on the benefits of the new feature, supported platforms, supported standards, and the commands necessary to configure the MSDP MIB feature

This document includes the following sections:

Feature Overview

Multicast Source Discovery Protocol (MSDP) is a mechanism to connect multiple PIM sparse-mode (SM) domains. MSDP allows multicast sources for a group to be known to all rendezvous points (RPs) in different domains. Each PIM-SM domain uses its own RPs and need not depend on RPs in other domains. An RP runs MSDP over TCP to discover multicast sources in other domains. MSDP support was implemented in Cisco IOS releases 12.0(5)S and 12.0(7)T.

The MSDP MIB describes managed objects that can be used to remotely monitor MSDP speakers using SNMP.

The MSDP MIB module contains four scalar objects and three tables. The tables are the Requests table, the Peer Table, and the Source-Active (SA) Cache Table. The Cisco implementation supports the Peer Table and SA Cache Table only. The Requests table contains information used to determine which peer to send SA requests to. However, the MSDP implementation used in Cisco IOS software does not associate sending SA requests to peers with group addresses (or group address masks).

Benefits

Allows the monitoring of devices in multiple PIM sparce-mode domains through a network management system (NMS).

Restrictions

All MSDP objects are implemented as read-only.

The Requests Table is not used in the MSDP MIB.

Related Features and Technologies

- Simple Network Management Protocol (SNMP)
- Multicast Source Discovery Protocol (MSDP)

Related Documents

For information on MSDP and the MSDP MIB, see the following Internet Draft documents (available at www.ietf.org):

- Fenner, B., and Thaler, D., “Multicast Source Discovery Protocol MIB”, Internet Draft, December 1999. [draft-ietf-msdp-mib-04.txt]
- Farinacci, D., Rekhter, Y., Meyer, D., Lothberg, P., Kilmer, H., and Hall, J., “Multicast Source Discovery Protocol”, Internet Draft, July 2000. [draft-ietf-msdp-spec-06.txt]

For information on configuring MSDP on your Cisco devices, see the 12.0(7)T feature guide titled “Multicast Source Discovery Protocol,” available on Cisco Connection Online.

For information on configuring SNMP using Cisco IOS software, see the following documents:

- The "Monitoring the Router and Network" chapter of the Release 12.0 *Cisco IOS Configuration Fundamentals Configuration Guide*
- The "Router and Network Monitoring Commands" chapter of the Release 12.0 *Cisco IOS Configuration Fundamentals Command Reference*.

For information on utilizing SNMP MIB features, see the appropriate documentation for your network management system.

For a complete implementation details of the MSDP MIB, see the file MSDP-MIB.my, available on your routing device, or from Cisco Connection Online (CCO) at http://www.cisco.com/public/mibs/v2/.

Supported Platforms

- Cisco 7200 series
- Cisco 7500 series (including 7000RSP platforms)
- Cisco 12000 series GSR

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

This feature introduces the MSDP MIB.

The MSDP-MIB.my file can be downloaded from the Cisco MIB web site on CCO at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

RFCs

The MSDP MIB is, at the time of the release of Cisco IOS Version 12.1(12)S, an "Internet Draft," and has not yet been given an RFC classification by the Internet Engineering Task Force (IETF).

Prerequisites

The tasks in this document assume you have configured SNMP and MSDP on your devices.

In each PIM-SM domain there should be a device configured as the speaker. This device must have SNMP enabled and have the MSDP MIB available.

All MSDP speakers should have an IP address configured in order to support SNMP Get operations.

Configuration Tasks

See the following sections for configuration tasks for the HSRP MIB feature. Each task in the list indicates if the task is optional or required.

- Configuring MSDP MIB Notifications (Required)
- Verifying MSDP MIB Configuration (Optional)
- Troubleshooting Tips (Optional)

Configuring MSDP MIB Notifications

To control the generation of MSDP traps or informs on a device, use any of the following commands in global configuration mode:

Command	Purpose
`Router# snmp-server enable traps msdp`	Enables the sending of MSDP notifications for use with SNMP. The **snmp-server enable traps** command enables both traps and informs.

Command	Purpose
`Router# no snmp-server enable traps msdp`	Disables the sending of MSDP notifications. The **no snmp-server enable traps** command disables both traps and informs.
`Router# snmp-server host host [traps | informs] [version {1 | 2c | 3 [auth | priv | noauth ]}] community-string [udp-port port-number] msdp`	Specifies the recipient (host) for MSDP traps or informs.

Verifying MSDP MIB Configuration

Use the **more system:running-config** or **show running-config** command to verify that the desired snmp-server commands are in your configuration file.

Troubleshooting Tips

You can compare the results of MSDP MIB notifications to output from the Cisco IOS software by using the **show ip msdp summary** and **show ip msdp peer** CLI commands on the appropriate routing device. You can verify Source-Active (SA) Cache Table entries using the **show ip msdp sa-cache** Cisco IOS CLI command.

Monitoring and Maintaining MSDP

The MSDP MIB feature is designed to provide information to network management applications (typically graphical-user-interface programs running on an external network management system). MSDP MIB objects can be read by the NMS using SNMP Get, Get-next, and Get-bulk operations.

Configuration Examples

The following example shows a configuration session on one of the Cisco devices serving as a speaker in a PIM sparce-mode domain. MSDP MIB traps are enabled to be sent to the host specified by the name myhost.cisco.com. The community string is defined as public.

```
Router# configure terminal
Router(config)# snmp-server community public ro
Router(config)# snmp-server enable traps msdp
Router(config)# snmp-server host myhost.cisco.com traps version 2c public msdp
```

Command Reference

This section documents the following modified commands:

- **snmp-server enable traps**
- **snmp-server host**

All other commands used with this feature are documented in the Cisco IOS Release 12.0 command reference publications.

snmp-server enable traps

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

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

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

Syntax Description

notification-type	(Optional) Type of notification to enable or disable. If no type is specified, all notifications supported on your routing device are enabled or disabled. Not all notification types are available for all Cisco platforms. The notification type can be one of the following keywords: • **bgp**—Controls (enables or disables) Border Gateway Protocol (BGP) state change notifications. • **config**—Controls configuration notifications. • **entity**—Controls Entity MIB modification notifications. • **envmon**—Controls Cisco enterprise-specific environmental monitor notifications. Notifications are sent when an environmental threshold is exceeded. When the **envmon** keyword is used, you can specify a *notification-option* value. • **frame-relay**—Controls Frame Relay notifications. • **hsrp**—Controls Hot Standby Routing Protocol (HSRP) notifications. • **isdn**—Controls Integrated Services Digital Network (ISDN) notifications. When the **isdn** keyword is used on Cisco 1600 series routers, you can specify a *notification-option* value. • **msdp**—Controls Multicast Source Discovery Protocol (MSDP) notifications. • **repeater**—Controls Ethernet hub repeater notifications. When the **repeater** keyword is selected, you can specify a *notification-option* value. • **rtr**—Controls response time reporter (RTR) notifications. • **snmp**—Controls Simple Network Management Protocol (SNMP) notifications (defined in RFC 1157). The following notification types are controlled by the **snmp-server enable traps snmp** command: authentication, linkup, linkdown, coldstart, and warmstart. You can use the **authentication** keyword to specifically enable or disable authentication notifications (see below). • **syslog**—Controls Cisco Syslog MIB error message notifications. Specify the level of messages to be sent with the **logging history level** command.

notification-option	• **envmon [voltage | shutdown | supply | fan | temperature]** When the **envmon** keyword is used, you can enable a specific environmental notification type, or accept all notification types from the environmental monitor system. If no option is specified, all environmental notifications are enabled. The option can be one or more of the following keywords: **voltage**, **shutdown**, **supply**, **fan**, and **temperature**. • **isdn [call-information | isdn u-interface]** When the **isdn** keyword is used, you can specify the call-information keyword to enable an SNMP ISDN call information notification for the ISDN MIB subsystem, or you can specify the **isdn u-interface** keyword to enable an SNMP ISDN U interface notification for the ISDN U interface MIB subsystem. • **repeater [health | reset]** 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 either of the following keywords: – **health**—Enables Repeater Hub MIB health notification. – **reset**—Enables Repeater Hub MIB reset notification. • **snmp [authentication]** When the **snmp** keyword is used, you can specify the **authentication** option to specifically enable or disable SNMP Authentication Failure notifications. (The **snmp-sever enable traps snmp authentication** command replaces the **snmp-server trap-authentication** command.) If no option is specified, all SNMP notifications are enabled. For definitions of SNMP notification types, see RFC 1157.

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, linkUp/linkDown notifications for specific interfaces 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 Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.0(12)S	The following keywords were added for the 12.0 S train: • **hsrp** • **msdp**

Usage Guidelines

This command is useful for disabling notifications that are generating 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 in conjunction with the **snmp-server host** command. Use 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 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 notifications cannot be controlled using the **snmp-server enable traps** command.

Examples

The following example sends MSDP MIB traps to the host specified by the name myhost.cisco.com. The community string is defined as public.

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

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

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

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

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

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

```
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

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server informs	Specifies inform request options.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server host

To specify the recipient of an SNMP notification operation, use the **snmp-server host** global configuration command. To remove the specified host from the configuration, use the **no** form of this command.

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

no snmp-server host *host* [**traps** | **informs**] [*notification-type*]

Syntax Description

host	Name or Internet address of the host.
traps	(Optional) Send SNMP traps to this host. This is the default.
informs	(Optional) Send SNMP informs to this host.
version	(Optional) Version of the Simple Network Management Protocol (SNMP) used to send the traps. • **1**—SNMPv1. This option is the default, and is not available with informs. • **2c**—SNMPv2c (also refered to as SNMPv2p). • **3**—SNMPv3 – **auth**—(Optional) Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication. – **priv**—(Optional) Enables Data Encryption Standard (DES) packet encryption (also called privacy). – **noauth**—(Optional)Specifies that no authentication checking is necessary. **Note**: If you specify SNMPv3 without the **auth** or **priv** keywords, the noAuthNoPriv security level is assumed.
community-string	Password-like community string sent with the notification operation.
udp-port *port*	(Optional) UDP port of the host to use. The default is 162.

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

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 to the host. No informs will be sent to this host.

If no **version** keyword is present, the default is version 1. If no **traps** or **informs** keyword is present, traps are enabled.

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

Command Modes Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.1(3)T	The **hsrp** keyword was added for the Cisco IOS Release 12.1 T train.
12.0(12)S	The following keywords were integrated in the Cisco IOS Release 12.0 S train: • **hsrp** • **msdp**

Usage Guidelines 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 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, while an inform may 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 will be 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 will replace the first.

The **snmp-server host** command is used in conjunction with the **snmp-server enable** command. Use 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.

A notification type option's availability depends on the router type and Cisco IOS software features supported on the router. For example, the **envmon** notification type is available only if the environmental monitor is part of the system (for example, the Cisco 12000 series GSR platforms use the environmental monitor).

Examples

The following example sends HSRP MIB traps to the host specified by the name myhost.cisco.com. The community string is defined as public.

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

The following example sends the SNMP traps defined in RFC 1157 to the host specified by the name myhost.cisco.com. The community string is defined as comaccess.

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

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

```
snmp-server enable traps
snmp-server host 172.30.2.160 public snmp envmon
```

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

```
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

Command	Description
snmp-server enable traps	Enables the sending of SNMP traps and informs.
snmp-server informs	Specifies inform request options.
snmp-server trap-source	Specifies the interface (and hence the corresponding IP address) that an SNMP trap should originate from.
snmp-server trap-timeout	Defines how often the system should try resending trap messages.

Glossary

inform—An SNMP trap message which includes a delivery confirmation request. See "trap."

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 using SNMP commands, usually through a Network Management System (NMS). MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

MSDP—Multicast Source Discovery Protocol. A mechanism to connect multiple PIM sparse-mode (SM) domains. MSDP allows multicast sources for a group to be known to all rendezvous point(s) (RPs) in different domains. Each PIM-SM domain uses its own RPs and need not depend on RPs in other domains. An RP runs MSDP over TCP to discover multicast sources in other domains.

Multicast Source Discovery Protocol—See MSDP.

NMS—Network Management System. An application or suite of applications designed to monitor networks using SNMP. CiscoView is one example of an NMS.

OID—Object Identifier. The values for OIDs are defined in specific MIB modules.

PDU—Protocol Data Unit. Refers to the information contained in an SNMP message. The SNMP PDU type identifies the type of message (trap or inform) being sent.

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.

trap—Message sent by an SNMP agent to a network management station, console, or terminal to indicate the occurrence of a significant event, such as a specifically defined condition or a threshold that was reached.