



MSDP MIB

This feature module describes the MSDP MIB support added for SNMP network monitoring in Cisco IOS Release 12.1(5)T. It includes the following sections:

- Feature Overview, page 1
- Supported Platforms, page 2
- Supported Standards, MIBs, and RFCs, page 3
- Prerequisites, page 3
- Configuration Tasks, page 4
- Monitoring and Maintaining MSDP, page 5
- Configuration Examples, page 5
- Command Reference, page 5
- Glossary, page 14

Feature Overview

Multicast Source Discovery Protocol (MSDP) is a mechanism to connect multiple Protocol Independent Multicast sparse-mode (PIM-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 (or other MSDP SA originator) runs MSDP over TCP to discover multicast sources in other domains. MSDP support was implemented in Cisco IOS Release 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

This feature allows the monitoring of MSDP activity using SNMP. Typically SNMP monitoring is performed using a Network Management System (NMS).

Restrictions

All MSDP-MIB objects are implemented as read-only.

The Requests table is not supported in Cisco's implementation of the MSDP MIB.

The msdpEstablished notification is not supported in Cisco's implementation of 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):

- “Multicast Source Discovery Protocol”, Internet Draft, July 2000 [draft-ietf-msdp-spec-06.txt]; Farinacci, D., Rekhter, Y., Meyer, D., Lothberg, P., Kilmer, H., and Hall, J.
- “Multicast Source Discovery Protocol MIB”, Internet Draft, December 1999 [draft-ietf-msdp-mib-03.txt]; Fenner, B., and Thaler, D.
(Note that Cisco currently supports only Draft 3 of the MIB)

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

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

- The “Configuring Simple Network Management Protocol (SNMP)” chapter of the Release 12.1 *Cisco IOS Configuration Fundamentals Configuration Guide*
- The “SNMP Commands” chapter of the Release 12.1 *Cisco IOS Configuration Fundamentals Command Reference*

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

For complete implementation details of the MSDP MIB, see the file MSDP-MIB.my, available from Cisco.com at <http://www.cisco.com/public/mibs/v2/>.

Supported Platforms

MSDP MIB functionality is available only in software images that support MSDP, IP multicast, and SNMP. Supported platforms include:

- Cisco 800 series
- Cisco 1400 series
- Cisco 1600 series
- Cisco 1700 series
- Cisco 2500 series

- Cisco 2600 series
- Cisco 3600 series
- Cisco 4500 series and Cisco 4700 series
- Cisco 6400
- Cisco 7000 family (Cisco 7100 series, 7200 series, and 7500 series)
- Cisco AS5300
- Cisco AS5400
- Cisco AS5800
- Cisco MC3810
- Cisco uBR7200 series
- Cisco MGX8850

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

- RFC2362; “Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification”
- MSDP and the MSDP MIB are, at the time of the release of Cisco IOS Version 12.1(5)T, Internet Drafts and have not yet been given an RFC classification by the Internet Engineering Task Force (IETF).

Prerequisites

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

In each PIM-SM domain there should be a device that is configured as the MSDP speaker. This device must have SNMP enabled and must 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 MSDP MIB feature. Each task in the list is identified as 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.
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.

Note that MSDP MIB notifications do not have to be enabled on a system to process simple Set or Get SNMP requests.

Verifying MSDP MIB Configuration

Use the **more system:running-config** or the **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 the 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 also compare the results of these commands to the results from SNMP Get operations. You can verify Source-Active (SA) Cache table entries using the **show ip msdp sa-cache** Cisco IOS CLI command. Additional troubleshooting information, such as the local address of the connection, the local port, and the remote port, and be obtained using the output from the **debug ip msdp** 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-SM 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 12.1 command reference publications.

snmp-server enable traps

To enable the router to send Simple Network Management Protocol (SNMP) traps or informs (notifications), use the **snmp-server enable traps** global configuration command. To disable SNMP notifications, use the **no** form of this command.

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

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

Syntax Description

<i>notification-type</i>	<p>(Optional) Type of notification to enable. If no type is specified, all available notifications are enabled. Note that the notification types available on your system will vary depending on platform support. The notification type can be one of the following keywords:</p> <ul style="list-style-type: none"> • bgp—Controls Border Gateway Protocol (BGP) state change notifications. • config—Controls SNMP configuration notifications. • dial—Controls SNMP dial control 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 <i>notification-option</i> value. • frame-relay—Controls Frame Relay notifications. • hsrp—Controls Hot Standby Router Protocol (HSRP) notifications as defined in the HSRP MIB. • isdn—Controls Integrated Services Digital Network (ISDN) notifications. When the isdn keyword is used, you can specify a <i>notification-option</i> value. • msdp—Controls Multicast Source Discovery Protocol (MSDP) notifications. • repeater—Controls Ethernet hub repeater notifications. When the repeater keyword is used, you can specify a <i>notification-option</i> value. • rsvp—Controls Resource Reservation Protocol (RSVP) notifications as defined in the RSVP MIB. • rtr—Controls Cisco Service Assurance Agent response time reporter (RTR) notifications. • snmp—Controls Simple Network Management Protocol (SNMP) notifications. When the snmp keyword is used, you can optionally specify a <i>notification-option</i> value. • syslog—Controls error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the logging history level command.
--------------------------	---

-
- notification-option* (Optional) Certain notification types have additional configuration options.
- **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 **isdnu-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 one or more of the following keywords:
 - **health**—Enables Repeater Hub MIB health notification.
 - **reset**—Enables Repeater Hub MIB reset notification.
 - **snmp** [**authentication** | **linkup** | **linkdown** | **coldstart**]
—(Optional) When the **snmp** keyword is used, you can specify the specific notification type you wish to enable or disable. If no keyword is used, all SNMP notification types are enabled (or disabled, if the **no** form is used). The notification types available are:
 - **authentication**—Controls the sending of SNMP authentication failure notifications. An authenticationFailure(4) trap signifies that the sending protocol entity is the addressee of a protocol message that is not properly authenticated.
 - **linkup**—Controls the sending of SNMP linkup notifications. A linkUp(3) trap signifies that the sending protocol entity recognizes that one of the communication links represented in the agent's configuration has come up.
 - **linkdown**—Controls the sending of SNMP linkdown notifications. A linkDown(2) trap signifies that the sending protocol entity recognizes a failure in one of the communication links represented in the agent's configuration.
 - **coldstart**—Controls the sending of SNMP coldstart notifications. A coldStart(0) trap signifies that the sending protocol entity is reinitializing itself such that the agent's configuration or the protocol entity implementation may be altered.
-

Defaults

SNMP notifications are disabled.

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

Command Modes Global configuration

Command History	Release	Modification
	11.1	This command was introduced.
	12.0(2)T	The rsvp keyword was added.
	12.0(3)T	The hsrp keyword was added.
	12.1(3)T	The following keywords were added to the snmp-server enable traps snmp form of this command: <ul style="list-style-type: none"> • linkup • linkdown • coldstart <p>The following notification type keywords were added for the Cisco AS5300 platform only:</p> <ul style="list-style-type: none"> • ds0-busyout • isdn chan-not-avail • modem-health • ds1-loopback <p>The following notification type keyword was added for the Cisco AS5300 and AS5800 platforms only:</p> <ul style="list-style-type: none"> • aaa-server
	12.1(5)T	The msdp keyword was added.

Usage Guidelines

The **no** form of the **snmp-server enable traps** command is useful for disabling notifications that are generating a large amount of unneeded noise on your network.

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. The notification types available on your routing device will vary depending on the Cisco IOS software image.

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 enabled or disabled (for example, HSRP traps are defined using the HSRP MIB, repeater traps are defined using the Repeater Hub MIB, and so on). Not all of the notification types available in the **snmp-server host** command have notificationEnable MIB objects, so some notification types cannot be controlled using the **snmp-server enable traps** command.

Examples

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

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

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

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

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

```
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 defined as public:

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

The following example sends HSRP MIB traps to the host myhost.cisco.com using the community string public.

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

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 a Simple Network Management Protocol (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

<i>host</i>	Name or Internet address of the host.
traps	(Optional) Sends SNMP traps to this host. This is the default.
informs	(Optional) Sends SNMP informs to this host.
version	(Optional) Version of SNMP used to send the traps. <ul style="list-style-type: none"> • 1—SNMPv1. This option is the default and is not available with informs. • 2c—SNMPv2c (also referred to as SNMPv2p to differentiate it from SNMPv2 Classic). • 3—SNMPv3. <ul style="list-style-type: none"> – 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. <p>Note: If you specify SNMPv3 without the auth or priv keywords, the noAuthNoPriv security level is assumed.</p>
<i>community-string</i>	Password-like community string sent with the notification operation.
udp-port <i>port-number</i>	(Optional) UDP port of the host to use. The default is 162.

<i>notification-type</i>	<p>(Optional) Type of notification to be sent to the host. If no type is specified, all available notifications are sent. The notification type can be one or more of the following keywords:</p> <ul style="list-style-type: none"> • 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. • frame-relay—Controls Frame Relay notifications. • hsrp—Controls Hot Standby Router 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. • rprr—Controls standard repeater (hub) notifications. • rsrb—Controls remote source-route bridging (RSRB) notifications. • rtr—Controls Cisco 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 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 specified 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.
12.1(5)T	The msdp keyword was added.

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 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, 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 informs** command for a host and then enter another **snmp-server host informs** 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.

The availability of a notification type option 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 “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 “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.”

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.

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.

PIM—Protocol Independent Multicast. Multicast routing architecture that allows the addition of IP multicast routing on existing IP networks. PIM is unicast routing protocol independent and can be operated in two modes: PIM dense mode (PIM-DM) and PIM sparse mode (PIM-SM).

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.

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, typically through the use of a NMS.

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.