



DistributedDirector MIB Support

Feature History

Release	Modification
12.2(8)T	This feature was introduced.

This document describes DistributedDirector MIB support and the enhancements and modifications made to the Cisco IOS Simple Network Management Protocol (SNMP) infrastructure in order to support DistributedDirector in Cisco IOS Release 12.2(8)T. It includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 3](#)
- [Supported Standards, MIBs, and RFCs, page 4](#)
- [Prerequisites, page 4](#)
- [Configuration Tasks, page 4](#)
- [Configuration Examples, page 6](#)
- [Command Reference, page 7](#)

Feature Overview

Network management takes place between two major types of systems: those in control, called managing systems, and those observed and controlled, called managed systems. The most common type of managing system is called a *network management system* (NMS). Managed systems can include hosts, servers, or network components such as routers or intelligent repeaters.

To promote interoperability, cooperating systems must adhere to a common framework and a common language, called a *protocol*. In the Internet network management framework, that protocol is the SNMP.

In a managed device, specialized low-impact software modules, called *agents*, access information about the device and make it available to the NMS. Managed devices maintain values for a number of variables and report those, as required, to the NMS. For example, an agent might report such data as the number of bytes and packets passing in and out of the device, or the number of broadcast messages sent and received. In the Internet network management framework, each variable is referred to as a *managed object*, which is anything that an agent can access and report back to the NMS.

All managed objects are contained in the Management Information Base (MIB), which is a database of the managed objects. The managed objects, or variables, can be set or read to provide information on network devices and interfaces. An NMS can control a managed device by sending a message to an agent of that managed device requiring the device to change the value of one or more of its variables.

The Cisco DistributedDirector MIB provides MIB support for DistributedDirector. This MIB contains DistributedDirector statistics, configurations, and status.

The DistributedDirector MIB contains five groups of object type definitions:

- `ciscoDistDirGeneralGroup`—A group of objects related to DistributedDirector general configurations, statistics, and status.
- `ciscoDistDirHostGroup`—A group of objects related to DistributedDirector host-specific configurations, statistics, and status.
- `ciscoDistDirServerGroup`—A group of objects related to DistributedDirector server-specific configurations, statistics, and status.
- `ciscoDistDirMappingGroup`—A group of objects related to associations between DistributedDirector host names and real servers.
- `ciscoDistDirNotificatonGroup`—A group of objects related to DistributedDirector significant events.

The DistributedDirector MIB defines the following tables:

- `cddGeneralMetricProfTable`—DistributedDirector metric profiles. A profile contains priority and weight values of DistributedDirector metrics, which can be applied to specific hosts or to the DistributedDirector default configuration.
- `cddHostTable`—DistributedDirector virtual host name or subdomain-specific configurations, statistics, and status entries.
- `cddHostConnectCfgTable`—DistributedDirector per-host server connect test configuration information entries.
- `cddHostTolCfgTable`—DistributedDirector per-host priority-level metric tolerance configuration information entries.
- `cddServerTable`—DistributedDirector server-specific information entries. This information includes the configuration parameters and statistics for each server.
- `cddServerPortTable`—DistributedDirector server port-specific information entries. This information includes the configuration parameters, statistics, and availability status for each service port on servers.
- `cddServerPortMetricTable`—DistributedDirector per-service per-metric weight entries.
- `cddHostServerMappingTable`—DistributedDirector associations of virtual host name to real server.

The DistributedDirector MIB defines the following notifications:

- `ciscoDistDirEventServerUp`—This trap is generated whenever a distributed server changes to the “up” state.
- `ciscoDistDirEventServerDown`—This trap is generated whenever a distributed server changes to the “down” state.
- `ciscoDistDirEventHitRateHigh`—This trap is generated whenever the incoming Domain Name system (DNS) HTTP query rate reaches a certain threshold. Use the Event MIB described in RFC 2981 to control the trigger of this notification.

The `ciscoDistDirEventServerUp` and `ciscoDistDirEventServerDown` notifications can be enabled or disabled using the Cisco IOS `snmp-server enable traps director` and `snmp-server host` commands.

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

Benefits

The DistributedDirector MIB provides network management functionality to DistributedDirector.

Restrictions

The DistributedDirector MIB implementation for Cisco IOS Release 12.2(8)T supports read-only capability to the objects defined in the MIB.

Related Features and Technologies

- Event MIB
- SNMP
- Network management

Related Documents

- The “Configuring SNMP Support” chapter of *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.2
- The “SNMP Commands” chapter of *Cisco IOS Configuration Fundamentals Command Reference*, Release 12.2
- RFC 1157, “Simple Network Management Protocol”
- Event MIB: RFC 2981, *Event MIB*

Supported Platforms

- Cisco 2600 series
- Cisco 3620 series
- Cisco 3640 series
- Cisco 3660 series
- Cisco 7200 series

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

- Cisco DistributedDirector MIB (CISCO-DIST-DIRECTOR-MIB.my)
- Event MIB (EVENT-MIB.my)

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

RFCs

- Event MIB: RFC 2981, *Event MIB*

Prerequisites

DistributedDirector must be running on the router.

Configuration Tasks

See the following sections for configuration tasks for the DistributedDirector MIB support feature. Each task in the list is identified as either required or optional.

- [Enabling DistributedDirector SNMP Notifications](#) (required)
- [Specifying the Recipient of an SNMP Notification](#) (required)

Enabling DistributedDirector SNMP Notifications

To enable DistributedDirector SNMP notifications, use the following command in global configuration mode:

Command	Purpose
Router(config)# snmp-server enable traps director	Enables DistributedDirector SNMP notifications.

To disable DistributedDirector SNMP notifications, use the following command in global configuration mode:

Command	Purpose
Router(config)# no snmp-server enable traps director	Disables DistributedDirector SNMP notifications.

Specifying the Recipient of an SNMP Notification

To specify the recipient of a DistributedDirector SNMP notification, use the following command in global configuration mode:

Command	Purpose
Router(config)# snmp-server host 10.0.0.1 public director	Specifies the recipient of a DistributedDirector SNMP notification, where the host 10.0.0.1 is using the community string defined as “public.”

To remove the specified recipient, use the following command in global configuration mode:

Command	Purpose
Router(config)# no snmp-server host host-address director	Removes the recipient of a DistributedDirector SNMP notification.

Verifying DistributedDirector Notification Information

Enter the **show running-config** command to verify that DistributedDirector SNMP notification information is configured. Both server up and server down information is included, unless you specify one or the other.

```
Router# show running-config

ip host myhost 172.2.2.10 172.2.2.20 172.2.2.30
.
.
.
snmp-server enable traps director server-up server-down
```

Configuration Examples

This section provides the following configuration examples:

- Enabling DistributedDirector SNMP Notifications Example
- Specifying the Recipient of an SNMP Notification Example

Enabling DistributedDirector SNMP Notifications Example

In the following example, both `ciscoDistDirEventServerUp` and `ciscoDistDirEventServerDown` notifications are enabled:

```
Router(config)# snmp-server enable traps director

Router# show running-config

ip host myhost 172.2.2.10 172.2.2.20 172.2.2.30
.
.
.
snmp-server enable traps director server-up server-down
```

Specifying the Recipient of an SNMP Notification Example

In the following example, the `ciscoDistDirEventServerUp` and `ciscoDistDirEventServerDown` notifications are to be sent to the host 10.0.0.1 using the community string defined as “public”:

```
Router(config)# snmp-server host 10.0.0.1 public director

Router# show snmp

Chassis:8768490
0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs
0 SNMP packets output
  0 Too big errors (Maximum packet size 1500)
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Response PDUs
  0 Trap PDUs

SNMP logging:enabled
Logging to 10.0.0.1.162, 0/10, 0 sent, 0 dropped.
```

Command Reference

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

- [snmp-server enable traps director](#)
- [snmp-server host](#)

snmp-server enable traps director

To enable DistributedDirector Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps director** command in global configuration mode. To disable DistributedDirector SNMP notifications, use the **no** form of this command.

snmp-server enable traps director [server-up | server-down]

no snmp-server enable traps director [server-up | server-down]

Syntax Description

<i>server-up</i>	(Optional) Enables the DistributedDirector notification that the server has changed to the “up” state.
<i>server-down</i>	(Optional) Enables the DistributedDirector notification that the server has changed to the “down” state.

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) DistributedDirector status notifications for systems. If none of the optional keywords is specified, all available environmental notifications are enabled.

Examples

In the following example, both `ciscoDistDirEventServerUp` and `ciscoDistDirEventServerDown` notifications are enabled:

```
Router(config)# snmp-server enable traps director

Router# show running-config

ip host myhost 172.2.2.10 172.2.2.20 172.2.2.30
.
.
.
ip director host myhost
ip dns primary myhost soa myhost myhost@com
ip director host myhost priority boomerang 1
no ip director drp synchronized
snmp-server enable traps director server-up server-down
```

Related Commands

Command	Description
snmp-server enable traps	Enables the router to send SNMP traps.
snmp-server host	Specifies the recipient of an SNMP notification.
snmp-server informs	Specifies inform request options.
snmp-server trap-source	Specifies the interface (and hence the corresponding IP address) from which an SNMP trap should originate.
snmp-server trap-timeout	Defines how often to try resending trap messages on the retransmission queue.
snmp trap link-status	Enables SNMP trap notifications to be generated when a specific port is brought up or down.

snmp-server host

To specify the recipient of a Simple Network Management Protocol (SNMP) notification, use the **snmp-server host** command in global configuration mode. To remove the specified recipient, use the **no** form of this command.

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

```
no snmp-server host host-address [traps | informs]
```

Syntax Description

<i>host-address</i>	Name or Internet address of the host (the targeted recipient).
traps	(Optional) Sends SNMP traps to this host. This is the default.
informs	(Optional) Sends SNMP informs to this host.
version	(Optional) Version of the SNMP used to send the traps. Version 3 is the most secure model because it allows packet encryption with the priv keyword. If you use the version keyword, one of the following keywords must be specified: <ul style="list-style-type: none"> • 1—SNMP Version 1. This option is not available with informs. • 2c—SNMP Version 2C. • 3—SNMP Version 3. One of the following three optional keywords can follow the 3 keyword: <ul style="list-style-type: none"> – auth—(Optional) Enables message digest 5 (MD5) algorithm and Secure Hash Algorithm (SHA) packet authentication. – noauth—(Optional) The noAuthNoPriv security level. This is the default if the [auth noauth priv] keyword choice is not specified. – priv—(Optional) Enables Data Encryption Standard (DES) packet encryption (also called “privacy”).
<i>community-string</i>	Password-like community string sent with the notification operation. Although you can set this string using the snmp-server host command by itself, we recommend that you define this string using the snmp-server community command prior to using the snmp-server host command.

udp-port <i>port</i>	(Optional) Specifies which user Datagram Protocol 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 notifications are sent. The notification type can be one or more of the following keywords:</p> <ul style="list-style-type: none"> • bgp—Sends Border Gateway Protocol (BGP) state change notifications. • config—Sends configuration notifications. • director—Sends DistributedDirector-related notifications to selected hosts. • dspu—Sends downstream physical unit (DSPU) notifications. • entity—Sends Entity MIB modification notifications. • envmon—Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded. • frame-relay—Sends Frame Relay notifications. • hsrp—Sends Hot Standby Router Protocol (HSRP) notifications. • ipsec—Sends IP Security (IPSec) notifications that are related to a MIB. • isdn—Sends ISDN notifications. • llc2—Sends Logical Link Control, type 2 (LLC2) notifications. • repeater—Sends standard repeater (hub) notifications. • rsrb—Sends remote source-route bridging (RSRB) notifications. • rsvp—Sends Resource Reservation Protocol (RSVP) notifications. • rtr—Sends Service Assurance Agent (response time reporter) notifications. • sdlc—Sends Synchronous Data Link Control (SDLC) notifications. • sdllc—Sends SDLC Logical Link Control notifications. • snmp—Sends SNMP notifications (as defined in RFC 1157). • stun—Sends serial tunnel (STUN) notifications. • syslog—Sends error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the logging history level command. • tty—Sends Cisco enterprise-specific notifications when a TCP connection closes. • x25—Sends X.25 event notifications.

Defaults

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(3)T	The following keywords were added: <ul style="list-style-type: none"> • version 3 [auth noauth priv] • hsrp
11.3(1) MA, 12.0(3)T	The voice notification-type keyword was added.
12.1(3)T	The calltracker notification-type keyword was added for the Cisco AS5300 and Cisco AS5800 platforms.
12.1(5a)E, 12.2(4)T	The ipsec notification-type keyword was added.
12.2(8)T	The director notification-type 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. If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destinations.

However, informs consume 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 may be retried several times. The retries increase traffic and contribute to higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. In order to configure the router to send 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.

In order 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 preceding command. Only the last-received **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 traps director** command. Use the **snmp-server enable traps director** command to specify which DistributedDirector SNMP notifications are sent globally. For a host to receive DistributedDirector notifications, the **snmp-server enable traps director** command and the **snmp-server host** command for that host must be enabled.

If no **version** keyword is present, the default is version 1. The **no snmp-server host** command with no keywords will disable traps, but not informs, to the host. In order to disable informs, use the **no snmp-server host informs** command.

**Note**

If the community-string is not defined using the **snmp-server community** command prior to using this command, the default form of the **snmp-server community** command will automatically be inserted into the configuration. The password (*community-string*) used for this automatic configuration of the **snmp-server community** command will be the same as that specified in the **snmp-server host** command.

Examples

If you want to configure a unique SNMP community string for traps, but you want to prevent access to SNMP polling with this string, the configuration should include an access list. In the following example, the community string is defined as “comaccess”, and the access list is numbered 10:

```
Router(config)# snmp-server community comaccess ro 10
Router(config)# snmp-server host 172.20.2.160 comaccess
Router(config)# access-list 10 deny any
!
Router(config)# snmp-server community comaccess RO 10
Router(config)# snmp-server enable traps director server-up server-down
Router(config)# snmp-server host 172.20.2.160 comaccess
Router(config)# snmp-server host 10.10.10.11 public director
```

In the following example, all available SNMP traps are enabled to be sent to the host specified by the name “myhost.cisco.com”. The community string is defined as “comaccess”.

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com comaccess snmp
```

In the following example, DistributedDirector MIB traps are enabled to be sent to the host “nms.cisco.com” using the community string defined as “public”:

```
Router(config)# snmp-server enable traps director
Router(config)# snmp-server host nms.cisco.com public director
```

Related Commands

Command	Description
snmp-server enable traps	Enables the router to send SNMP traps.
snmp-server enable traps director	Enables DistributedDirector SNMP notifications.
snmp-server informs	Specifies inform request options.
snmp-server trap-source	Specifies the interface (and hence the corresponding IP address) from which an SNMP trap should originate.
snmp-server trap-timeout	Defines how often to try resending trap messages on the retransmission queue.
snmp trap link-status	Enables SNMP trap notifications to be generated when a specific port is brought up or down.

