CISCO-FLASH-MIB Enhancements

The CISCO-FLASH-MIB Enhancements feature includes the following modifications:

- A new Flash card trap variable (varbind) has been added to the CISCO-FLASH-MIB ciscoFlashDeviceChange notification.
- Two notifications, one for insertion of a Flash card and one for removal of a Flash card, and file type support information have been added to the CISCO-FLASH-MIB.
- The command-line interface (CLI) has been modified to control the Flash card insertion and removal notifications.

Feature History for the CISCO-FLASH-MIB Enhancements Feature

Release	Modification
12.3(2)T	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for CISCO-FLASH-MIB Enhancements

- Your Cisco router must support CISCO-FLASH-MIB and be running Cisco IOS Release 12.3(2)T or later software.
- Before you can view CISCO-FLASH-MIB notifications or enable or disable Flash card notifications, you must first have installed a Cisco router-compatible Flash card.

Information About CISCO-FLASH-MIB Enhancements

This section contains the following concepts:

ciscoFlashDeviceSize As Varbind for ciscoFlashDeviceChangeTrap

The ciscoFlashDeviceChangeTrap notification is sent when a Flash card is inserted or removed from your system. The ciscoFlashDeviceSize varbind has been added to the notification to help you identify the size of the Flash card when it is inserted. The size is shown as a non-zero value of the Flash card. If the Flash card is removed, the value is shown as zero.

New Notifications for Flash Insertion and Removal

Two notifications have been added to the CISCO-FLASH-MIB. The following notification is sent when a Flash card is inserted in your system:

```
ciscoFlashDeviceInsertedNotif
```

The following notification is sent if a Flash card is removed from your system:

```
ciscoFlashDeviceRemoveNotif
```

CLI for Enabling Flash Notifications

Two commands have been modified so that you can enable and disable MIB Flash notifications on your device. Using the **snmp-server enable traps** command, you can enable all Simple Network Management Protocol (SNMP) notifications (traps or informs) that are available on your system. The **flash** notification type has been added as a keyword so that you can globally enable or disable Flash card insertion and removal notifications. The **snmp-server host** command allows you to specify the recipient of a notification. The **flash** notification type has been added to this command so that you can specify that Flash notifications be sent.

File Type Support in CISCO-FLASH-MIB

The object ciscoFlashFileType has been added to the CiscoFlashFileTable in the CISCO-FLASH-MIB so that you can determine the type of file that is stored in Flash memory.

How to Enable Flash Card Notifications

This section contains the following procedure:

- Enabling Flash Card Notifications, page 3

Enabling Flash Card Notifications

To enable Flash card notifications, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps flash** [**insertion**] [**removal**]
4. **snmp-server host** *host-address community-string* **flash**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

	Command or Action	Purpose
Step 3	**snmp-server enable traps flash** [**insertion**] [**removal**] **Example:** `Router (config)# snmp-server enable traps flash insertion`	Enables Simple Network Management Protocol (SNMP) Flash notifications. • **insertion—**Notifications will be sent for Flash card insertions. • **removal—**Notifications will be sent for Flash card removals. • If both **insertion** and **removal** are entered, notifications will be sent for both Flash card insertions and Flash card removals. • By default, Flash traps are turned off.
Step 4	**snmp-server host** *host-address community-string* **flash** **Example:** `Router (config)# snmp-server host 10.2.0.0 string123 flash`	Specifies the recipient of an SNMP notification operation and specifies the notification type as Flash.

Troubleshooting Tips

To verify the type of file that is stored in Flash memory, you can use the **show bootflash:** and **show flash** commands. (See the "Verifying the Type of File That Is Stored in Flash Memory: Example" section for sample output.)

Configuration Examples for Enabling Flash Notifications

This section contains the following configuration examples:

Enabling Flash Notifications: Example

The following example shows that Flash card notifications have been enabled for all Flash card insertions and deletions:

```
Router (config)# snmp-server enable traps flash insertion removal
Router (config)# snmp-server host 10.2.0.4 string45 flash
```

Verifying the Type of File That Is Stored in Flash Memory: Example

The following is sample output from the **show bootflash:** command. The file type is shown under the "type" column.

```
Router # show bootflash:
```

```
-#- ED --type-- --crc--- -seek-- nlen -length- -----date/time------ name
1   .. unknown  AC05EDDF  37A6B8   22  3384888 Dec 14 2000 00:02:15
c7200-boot-mz.120-4.XE
2   .. unknown  A74B5E65  37AC90   14     1365 May 02 2001 01:53:54
config/startup
       ^^^^^^
```

Verifying the Types of Notifications That Have Been Enabled: Example

In the following output example, the first ciscoFlashDeviceChangeTrap notification shows that a Flash card has been inserted. The second notification shows that a Flash card has been removed.

```
csipl-snmp:12> traprcv
Waiting for traps.

Received SNMPv2c Trap:
Community: public
From: 10.9.2.13
sysUpTimeInstance = 162720
snmpTrapOID.0 = ciscoFlashDeviceChangeTrap
ciscoFlashDeviceMinPartitionSize.2 = 20578304
ciscoFlashDeviceName.2 = slot1

Received SNMPv2c Trap:
Community: public
From: 10.9.2.13
sysUpTimeInstance = 162721
snmpTrapOID.0 = ciscoFlashDeviceInsertedNotif
ciscoFlashDeviceMinPartitionSize.2 = 20578304
ciscoFlashDeviceName.2 = slot1

Received SNMPv2c Trap:
Community: public
From: 10.9.2.13
sysUpTimeInstance = 163168
snmpTrapOID.0 = ciscoFlashDeviceChangeTrap
ciscoFlashDeviceMinPartitionSize.2 = 0
ciscoFlashDeviceName.2 = slot1
```

```
Received SNMPv2c Trap:
Community: public
From: 10.9.2.13
sysUpTimeInstance = 163169
snmpTrapOID.0 = ciscoFlashDeviceRemovedNotif
ciscoFlashDeviceName.2 = slot1
```

Additional References

For additional information related to CISCO-FLASH-MIB notifications, refer to the following references:

Related Documents

Related Topic	Document Title
Cisco MIBs	*Introduction to Cisco MIBs* at the Cisco.com website.
Cisco configuration fundamentals and network management commands	*Cisco IOS Configuration Fundamentals and Network Management Command Reference*, Release 12.3

Standards

Standards	Title
This feature has no new or modified standards.	–

MIBs

MIBs	MIBs Link
• CISCO-FLASH-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
This feature has no new or modified RFCs.	–

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.3 command reference publications.

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

snmp-server enable traps

To enable all Simple Network Management Protocol (SNMP) notifications (traps or informs) available on your system, use the **snmp-server enable traps** command in global configuration mode. To disable all available SNMP notifications, use the **no** form of this command.

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

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

Syntax Description

notification-type (Optional) Type of notification (trap or inform) to enable or disable. If no type is specified, all notifications available on your device are enabled or disabled. The notification type can be one of the following keywords:

- **config**—Controls configuration notifications, as defined in the CISCO-CONFIG-MAN-MIB (enterprise 1.3.6.1.4.1.9.9.43.2). The notification type is (1) ciscoConfigManEvent.
- **ds0-busyout**—Sends notification whenever the busyout of a DS0 interface changes state (Cisco AS5300 platform only). This notification is defined in the CISCO-POP-MGMT-MIB (enterprise 1.3.6.1.4.1.9.10.19.2) and the notification type is (1) cpmDS0BusyoutNotification
- **ds1-loopback**—Sends notification whenever the DS1 interface goes into loopback mode (Cisco AS5300 platform only). This notification type is defined in the CISCO-POP-MGMT-MIB (enterprise 1.3.6.1.4.1.9.10.19.2) as (2) cpmDS1LoopbackNotification.
- **entity**—Controls Entity MIB modification notifications. This notification type is defined in the ENTITY-MIB (enterprise 1.3.6.1.2.1.47.2) as (1) entConfigChange.
- **flash** [**insertion**] [**removal**]—Sends Flash notifications. Use the **insertion** keyword to send notifications when a Flash card is inserted. Use the **removal** keyword to send notifications when a Flash card is removed. Use both the **insertion** and **removal** keywords to send notifications for Flash card insertions and removals. By default, Flash traps are disabled.
- **hsrp**—Controls Hot Standby Routing Protocol (HSRP) notifications, as defined in the CISCO-HSRP-MIB (enterprise 1.3.6.1.4.1.9.9.106.2). The notification type is (1) cHsrpStateChange.
- **ipmulticast**—Controls IP Multicast notifications.
- **modem-health**—Controls modem-health notifications.
- **rsvp**—Controls Resource Reservation Protocol (RSVP) flow change notifications.
- **tty**—Controls TCP connection notifications.
- **xgcp**—Sends External Media Gateway Control Protocol (XGCP) notifications. This notification is from the XGCP-MIB-V1SMI.my and the notification is (1) xgcpUpDownNotification (enterprise 1.3.6.1.3.90.2).

Note For additional notification types, see the “Related Commands” section.

Defaults

This command is disabled by default. Most notification types are disabled. However, some notification types cannot be controlled with this 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
10.3	This command was introduced.
12.0(2)T	The **rsvp** keyword was added.
12.0(3)T	The **hsrp** keyword was added.
12.3(2)T	The **flash** [**insertion**] [**removal**] *notification-type* keywords were added.

Usage Guidelines

For additional notification types, see the "Related Commands" section for this command.

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. To specify whether the notifications should be sent as traps or informs, use the **snmp-server host** [**traps** | **informs**] command.

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.

Examples

The following example enables the router to send all traps to the host specified by the name myhost.cisco.com, using the community string defined as public:

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

The following example enables the router to send all inform requests to the host at the address myhost.cisco.com, using the community string defined as public:

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

```
Router(config)# snmp-server enable traps hsrp
Router(config)# snmp-server host myhost.cisco.com traps version 2c public hsrp
```

The following example specifies that Flash insertion notifications will be sent:

```
Router (config)# snmp-server enable traps flash insertion
```

Related Commands

Command	Description
snmp-server enable traps atm pvc	Controls (enables or disables) ATM PVC SNMP notifications.
snmp-server enable traps atm pvc extension	Enables the sending of extended ATM permanent virtual circuit (PVC) SNMP notifications.
snmp-server enable traps bgp	Controls (enables or disables) BGP server state change SNMP notifications.
snmp-server enable traps calltracker	Controls (enables or disables) Call Tracker callSetup and callTerminate SNMP notifications.
snmp-server enable traps envmon	Controls (enables or disables) environmental monitor SNMP notifications.
snmp-server enable traps frame-relay	Controls (enables or disables) Frame Relay DLCI link status change SNMP notifications.
snmp-server enable traps ipsec	Controls (enables or disables) IP Security SNMP notifications.
snmp-server enable traps isakmp	Controls (enables or disables) IPSec Internet Security Association and Key Exchange Protocol (ISAKMP) SNMP notifications.
snmp-server enable traps isdn	Controls (enables or disables) ISDN SNMP notifications.
snmp-server enable traps mpls ldp	Controls (enables or disables) MPLS Label Distribution Protocol (LDP) SNMP notifications.
snmp-server enable traps mpls traffic-eng	Controls (enables or disables) MPLS traffic engineering (TE) tunnel state-change SNMP notifications.
snmp-server enable traps mpls vpn	Controls (enables or disables) MPLS VPN specific SNMP notifications.
snmp-server enable traps repeater	Controls (enables or disables) RFC 1516 Hub notifications.
snmp-server enable traps snmp	Controls (enables or disables) RFC 1157 SNMP notifications.
snmp-server enable traps syslog	Controls (enables or disables) the sending of system logging messages via SNMP.
snmp-server host	Specifies whether you want the SNMP notifications sent as traps or informs, the version of SNMP to use, the security level of the notifications (for SNMPv3), and the destination host (recipient) for the notifications.
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 trap illegal-address	Issues an SNMP trap when a MAC address violation is detected on an Ethernet hub port of a Cisco 2505, Cisco 2507, or Cisco 2516 router.

snmp-server host

To specify the recipient of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** command in global configuration mode. To remove the specified host from the configuration, 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*] [**vrf** *vrf-name*]

no snmp-server host *host-address* [**traps** | **informs**] [**version** {**1** | **2c | 3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*] [**vrf** *vrf-name*]

Syntax Description

host-address	Name or Internet address of the host (the targeted recipient).
traps	(Optional) Specifies that notifications should be sent as traps. This is the default.
informs	(Optional) Specifies that notifications should be sent as informs.
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: • **1**—SNMPv1. This option is not available with informs. • **2c**—SNMPv2C. • **3**—SNMPv3. One of the following three optional keywords can follow the version 3 keyword: – **auth**—Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication. – **noauth**—Specifies that the noAuthNoPriv security level applies to this host. This is the default security level for SNMPv3. – **priv**—Enables Data Encryption Standard (DES) packet encryption (also called “privacy”).
community-string	Password-like community string sent with the notification operation. Though you can set this string using the **snmp-server host** command by itself, we recommend you define this string using the **snmp-server community** command prior to using the **snmp-server host** command.
up-port *port*	(Optional) User Datagram Protocol (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 available notifications are sent. The notification type can be one or more of the following keywords:

- **bgp**—Sends Border Gateway Protocol (BGP) state change notifications.
- **calltracker**—Sends Call Tracker call-start/call-end notifications.
- **config**—Sends configuration change notifications.
- **director**—Sends DistributedDirector-related notifications.
- **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.
- **flash**—Sends Flash card insertion and removal notifications.
- **frame-relay**—Sends Frame Relay notifications.
- **hsrp**—Sends Hot Standby Routing Protocol (HSRP) notifications.
- **ipmobile**—Sends Mobile IP notifications.
- **ipsec**—Sends IP Security (IPSec) notifications.
- **isdn**—Sends ISDN notifications.
- **llc2**—Sends Logical Link Control, type 2 (LLC2) notifications.
- **mpls-ldp**—Sends MPLS Label Distribution Protocol (LDP) notifications indicating status changes in LDP sessions.
- **mpls-traffic-eng**—Sends MPLS traffic engineering notifications indicating changes in the status of MPLS traffic engineering tunnels.
- **mpls-vpn**—Sends MPLS VPN notifications.
- **pim**—Sends Protocol Independent Multicast (PIM) 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 (RTR) notifications.
- **sdlc**—Sends Synchronous Data Link Control (SDLC) notifications.
- **sdllc**—Sends SDLC Logical Link Control (SDLLC) notifications.
- **snmp**—Sends any enabled RFC 1157 SNMP linkUp, linkDown, authenticationFailure, warmStart, and coldStart notifications.

Note To enable RFC 2233 compliant link up/down notifications, you should use the **snmp server link trap** command.

- **srp**—Sends Spatial Reuse Protocol (SRP) notifications.
- **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.

notification-type (Continued)	• **tty**—Sends Cisco enterprise-specific notifications when a TCP connection closes. • **voice**—Sends SNMP poor quality of voice traps, when used with the **snmp enable peer-trap poor qov** command. • **vsimaster—**Sends VSI Master notifications. • **x25**—Sends X.25 event notifications.
vrf *vrf-name*	(Optional) Specifies the Virtual Private Network (VPN) routing and forwarding (VRF) table that should be used to send SNMP 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 version 3 is specified, but the security level is not specified, the default security level is **noauth**.

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.

The default UDP port is 162.

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** will be the same as specified in the **snmp-server host** command. This is the default behavior for Cisco IOS Release 12.0(3) and later.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(3)T	The following keywords were added: • **version 3** [**auth** | **noauth** | **priv**] • **hsrp**
11.3(1)MA	The **voice** notification-type keyword was added.
12.0(3)T	The **voice** notification-type keyword was integrated into Release 12.0(3)T.
12.1(3)T	The **calltracker** notification-type keyword was added for the Cisco AS5300 and AS5800 platforms.
12.2(2)T	• The **vrf** *vrf-name* keyword/argument combination was added. • The **ipmobile** notification-type keyword was added. • Support for the **vsimaster** notification-type keyword was added for the Cisco 7200 and Cisco 7500 series.

Release	Modification
12.2(4)T	• The **pim** notification-type keyword was added. • The **ipsec** notification-type keyword was added.
12.2(8)T	• The **mpls-traffic-eng** notification-type keyword was added. (Also in 12.0(17)ST) • The **director** notification-type keyword was added.
12.2(13)T	• The **srp** notification-type keyword was added. • The **mpls-vpn** notification-type keyword was added. (Also in 12.0(22)S) • The **mpls-ldp** notification-type keyword was added.
12.3(2)T	The **flash** *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 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 are sent. 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.

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.

The availability of a notification-type 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. To see what notification types are available on your system, use the command help **?** at the end of the **snmp-server host** command.

The **vrf** keyword allows you to specify the notifications being sent to a specified IP address over a specific VRF. The VRF defines a VPN membership of a customer so that data is stored using the VPN.

Regarding Notification-Type Keywords

The *notification-type* keywords used in the **snmp-server host** command do not always match the keywords used in the corresponding **snmp-server enable traps** command. For example, the notification keyword applicable to MPLS traffic engineering tunnels is specified as **mpls-traffic-eng** (containing two dashes and no intervening spaces). The corresponding parameter in the **snmp-server enable traps** command is specified as **mpls traffic-eng** (containing an intervening space and a dash).

This syntax difference is necessary to ensure that the CLI interprets the *notification-type* keyword of the **snmp-server host** command as a unified, single-word construct, which preserves the capability of the **snmp-server host** command to accept multiple *notification-type* keywords in the CLI command line. The **snmp-server enable traps** commands, however, often use two-word constructs to provide hierarchical configuration options and to maintain consistency with the command syntax of related commands. Table 1 maps **snmp-server enable traps** commands to the keywords used in the **snmp-server host** command.

Table 1 Notification Keywords and Corresponding SNMP Enable Traps Commands

SNMP Enable Traps Command	SNMP Host Command Keyword
snmp-server enable traps mpls ldp	**mpls-ldp**
snmp-server enable traps mpls traffic-eng[1]	**mpls-traffic-eng**
snmp-server enable traps mpls vpn	**mpls-vpn**

1. See the *Cisco IOS Switching Services Command Reference* for documentation of this command.

Examples

If you want to configure a unique SNMP community string for traps, but you want to prevent SNMP polling access with this string, the configuration should include an access list. In the following example, the community string is named 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
```

The following example sends RFC 1157 SNMP traps to the host specified by the name myhost.cisco.com. Other traps are enabled, but only SNMP traps are sent because only **snmp** is specified in the **snmp-server host** command. The community string is defined as comaccess.

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

```
Router(config)# snmp-server enable traps snmp
Router(config)# snmp-server enable traps envmon
Router(config)# 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:

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

```
Router(config)# snmp-server enable traps bgp
Router(config)# 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:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

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

```
Router(config)# snmp-server enable traps hsrp
Router(config)# snmp-server host myhost.cisco.com informs version 2c public hsrp
```

The following example sends all SNMP notifications to xyz.com over the VRF named trap-vrf:

```
Router(config)# snmp-server host xyz.com vrf trap-vrf
```

The following example shows that Flash notifications are to be sent:

```
Router (config)# snmp-server host myhost.cisco.com string1 flash
```

Related Commands

Command	Description
snmp-server enable peer-trap poor qov	Enable poor quality of voice notifications for applicable calls associated with a specific voice dial peer.
snmp-server enable traps	Enables SNMP notifications (traps and informs).
snmp-server informs	Specifies inform request options.
snmp-server link trap	Enables linkUp/linkDown SNMP traps which are compliant with RFC 2233.
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 to try resending trap messages on the retransmission queue.