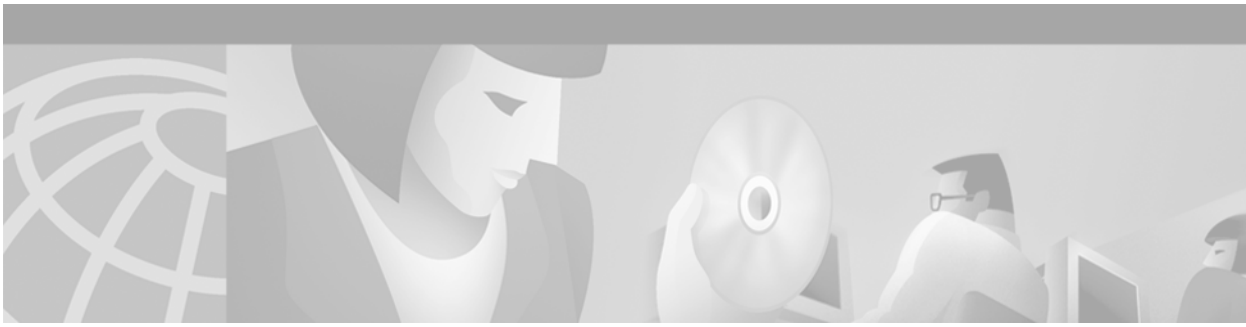


Configuring Simple Network Management Protocol (SNMP)

This chapter describes the Simple Network Management Protocol (SNMP), SNMP Management Information Bases (MIBs), and how to configure SNMP on Cisco devices.

For a complete description of the router monitoring commands mentioned in this chapter, refer to the "SNMP Commands" chapter in the "System Management" part of the Release 12.1 *Cisco IOS Configuration Fundamentals Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

Understanding SNMP

The Simple Network Management Protocol (SNMP) system consists of the following three parts:

- An SNMP manager (client)
- An SNMP agent (server)
- A Management Information Base (MIB)

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents.

The SNMP manager can be part of a Network Management System (NMS) such as CiscoWorks. The agent and MIB reside on the router. To configure SNMP on the router, you define the relationship between the manager and the agent.

The Management Information Base (MIB) is a virtual information storage area for network management information, which consists of collections of managed objects. As explained in RFC 2570[1]: "Collections of related objects are defined in MIB modules. These modules are written in the SNMP MIB module language, which contains elements of OSI's Abstract Syntax Notation One (ASN.1) language. STD 58, RFC 2578, RFC 2579, and RFC 2580 together define the MIB module language, specify the base data types for objects, specify a core set of short-hand specifications for data types called textual conventions, and specify a few administrative assignments of object identifier (OID) values."

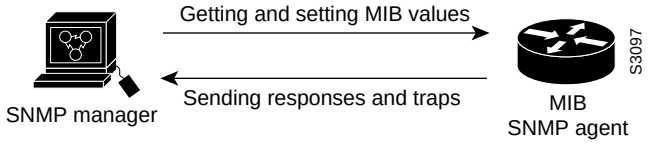
The SNMP agent contains MIB variables whose values the SNMP manager can request or change. A manager can get a value from an agent or store a value into that agent. The agent gathers data from the MIB, the repository for information about device parameters and network data. The agent can also respond to a manager's requests to get or set data.

1. RFC 2570: Copyright (C) The Internet Society (1998). All Rights Reserved.

An agent can send unsolicited traps to the manager. Traps are messages alerting the SNMP manager to a condition on the network. Traps can indicate improper user authentication, restarts, link status (up or down), closing of a TCP connection, loss of connection to a neighbor router, or other significant events.

Figure 17 illustrates the communications relationship between the SNMP manager and agent. A manager can send the agent requests to get and set MIB values. The agent can respond to these requests. Independent of this interaction, the agent can send unsolicited traps to the manager to notify the manager of network conditions.

Figure 17 Communication between an SNMP Agent and Manager



SNMP Notifications

The SNMP Inform Requests feature allows routers to send inform requests to SNMP managers.

Routers can send notifications to SNMP managers when particular events occur. For example, an agent router might send a message to a manager when the agent router experiences an error condition.

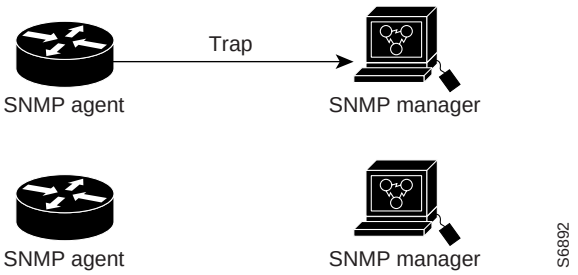
SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send any acknowledgment when it receives a trap. The sender cannot determine if the trap was received. However, an SNMP manager that receives an inform request acknowledges the message with an SNMP response PDU. If the manager does not receive an inform request, it does not send a response. If the sender never receives a response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.

Because they are more reliable, informs consume more resources in the router 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. Thus, traps and inform requests provide a trade-off between reliability and resources. If it is important that the SNMP manager receives every notification, use inform requests. On the other hand, if you are concerned about traffic on your network or memory in the router and you do not need to receive every notification, use traps.

Figure 18 through Figure 21 illustrate the differences between traps and inform requests.

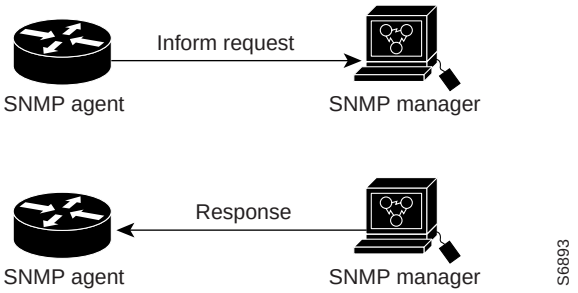
In Figure 18, the agent router successfully sends a trap to the SNMP manager. Although the manager receives the trap, it does not send any acknowledgment to the agent. The agent has no way of knowing that the trap reached its destination.

Figure 18 Trap Sent to SNMP Manager Successfully



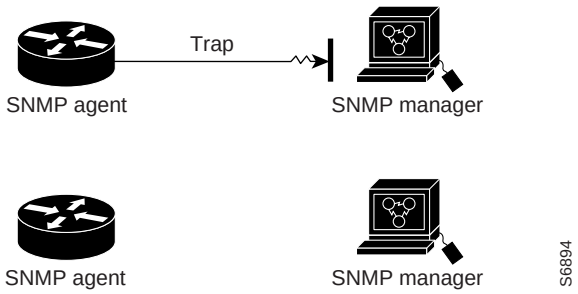
In Figure 19, the agent router successfully sends an inform request to the manager. When the manager receives the inform request, it sends a response back to the agent. Thus, the agent knows that the inform request successfully reached its destination. Notice that, in this example, twice as much traffic is generated as in Figure 18; however, the agent is sure that the manager received the notification.

Figure 19 Inform Request Sent to SNMP Manager Successfully



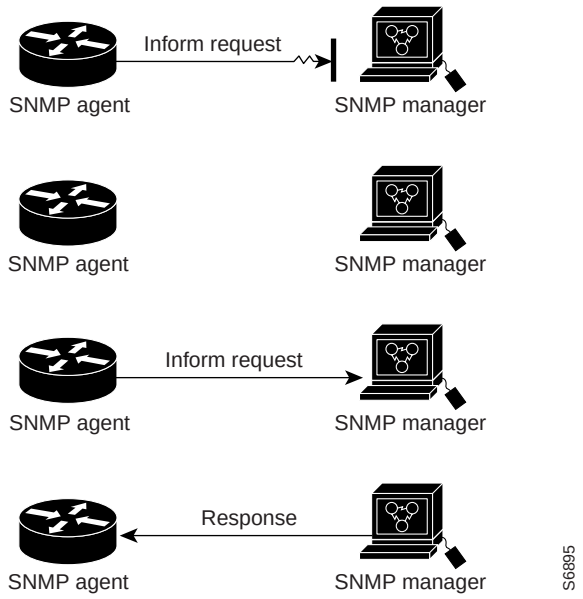
In Figure 20, the agent sends a trap to the manager, but the trap does not reach the manager. Since the agent has no way of knowing that the trap did not reach its destination, the trap is not sent again. The manager never receives the trap.

Figure 20 Trap Unsuccessfully Sent to SNMP Manager



In Figure 21, the agent sends an inform request to the manager, but the inform request does not reach the manager. Since the manager did not receive the inform request, it does not send a response. After a period of time, the agent will resend the inform request. The second time, the manager receives the inform request and replies with a response. In this example, there is more traffic than in Figure 20; however, the notification reaches the SNMP manager.

Figure 21 Inform Request Unsuccessfully Sent to SNMP Manager



Versions of SNMP

Cisco IOS Release 12.1 software supports the following versions of SNMP:

- SNMPv1—The Simple Network Management Protocol: A Full Internet Standard, defined in RFC 1157. (RFC 1157 replaces the earlier versions that were published as RFC 1067 and RFC 1098.) Security is based on community strings.
- SNMPv2c—The community-string based Administrative Framework for SNMPv2. SNMPv2c (the "C" stands for "community") is an Experimental Internet Protocol defined in RFC 1901, RFC 1905, and RFC 1906. SNMPv2c is an update of the protocol operations and data types of SNMPv2p (SNMPv2 Classic), and uses the community-based security model of SNMPv1.
- SNMPv3—Version 3 of the Simple Network Management Protocol. SNMPv3 is an interoperable standards-based protocol defined in RFCs 2273-2275. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network.

  The security features provided in SNMPv3 are:

  – Message integrity—Ensuring that a packet has not been tampered with in-transit.
  – Authentication—Determining the message is from a valid source.
  – Encryption—Scrambling the contents of a packet prevent it from being seen by an unauthorized source.

Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers able to access the agent's MIB is defined by an IP address access control list and password.

SNMPv2C support includes a bulk retrieval mechanism and more detailed error message reporting to management stations. The bulk retrieval mechanism supports the retrieval of tables and large quantities of information, minimizing the number of round-trips required. The SNMPv2C improved error handling support includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes now report the error type. Three kinds of exceptions are also reported: no such object exceptions, no such instance exceptions, and end of MIB view exceptions.

SNMPv3 is a security model.A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level will determine which security mechanism is employed when handling an SNMP packet. See Table 15 for a list of security levels available in SNMPv3.

Three security models are available: SNMPv1, SNMPv2c, and SNMPv3. Table 15 identifies what the combinations of security models and levels mean:

Table 15 SNMP Security Models and Levels

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community String	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	MD5 or SHA	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
v3	authPriv	MD5 or SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.

Note SNMPv2p (SNMPv2 Classic) is not supported in any Cisco IOS Releases after 11.2. SNMPv2C replaces the Party-based Administrative and Security Framework of SNMPv2p with a Community-based Administrative Framework. SNMPv2C retained the bulk retrieval and error handling capabilities of SNMPv2p.

You must configure the SNMP agent to use the version of SNMP supported by the management station. An agent can communicate with multiple managers; for this reason, you can configure the Cisco IOS software to support communications with one management station using the SNMPv1 protocol, one using the SNMPv2c protocol, and another using SMNPv3.

Supported MIBs and RFCs

Cisco's implementation of SNMP supports all MIB II variables (as described in RFC 1213) and defines all traps using the guidelines described in RFC 1215.Cisco provides its own private MIB extensions with every system.

The SNMPv3 feature supports RFCs 1901-1908, 2104, 2206, 2213, 2214, and 2271-2275. For additional information on SNMPv3, please see RFC 2570, "Introduction to Version 3 of the Internet-standard Network Management Framework" (please note that this is not a standards document).

For a list of descriptions of the supported RFCs, see the "References and Recommended Reading" appendix of the Release 12.1 *Cisco IOS Configuration Fundamentals Command Reference*. The full text for each RFC may be obtained from the World Wide Web at: http://www.rfc-editor.org/.

New MIB Support in Cisco IOS Release 12.1

Cisco IOS Release 12.1 adds support for the Resource Reservation Protocol (RSVP) MIB, the Integrated Services MIB, and the Integrated Services Guaranteed S.E. MIB (defined in RFCs 2206, 2213, and 2214, respectively). This support allows the use of **rsvp** as a *notification-type* in the **snmp-server enable traps** command. The RSVP MIB also specifies two traps (NetFlow and LostFlow) which are triggered when a new flow is created or deleted.

This release also adds support for the HSRP MIB (read only version), which allows use of **hsrp** as a *notification-type* in the **snmp-server enable traps** command, and in the **snmp-server host command**. For further HSRP-specific configuration information, see the "Configuring IP Services" chapter of the *Cisco IOS IP and IP Routing Configuration Guide*.

For a complete list of supported MIBs by platform and release, see the "Cisco MIBs" area of Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

SNMP Configuration Task List

There is no specific command that you use to enable SNMP. The first **snmp-server** command that you enter enables the supported versions of SNMP.

To configure SNMP support, perform any of the tasks in the following sections. The second task is required; all other tasks are optional.

- Creating or Modifying an SNMP View Record
- Creating or Modifying Access Control for an SNMP Community
- Specifying an SNMP-Server Engine Name (ID)
- Specifying SNMP-Server Group Names
- Configuring SNMP-Server Hosts
- Configuring SNMP-Server Users
- Enabling the SNMP Agent Shutdown Mechanism
- Establishing the Contact, Location, and Serial Number of the SNMP Agent
- Defining the Maximum SNMP Agent Packet Size
- Limiting TFTP Servers Used Via SNMP
- Monitoring SNMP Status
- Disabling the SNMP Agent
- Configuring SNMP Traps
- Enabling SNMP Informs
- Configuring the Router as an SNMP Manager

Creating or Modifying an SNMP View Record

You can assign views to community strings to limit which MIB objects an SNMP manager can access. You can use a predefined view, or create your own view. If you are using a predefined view or no view at all, skip this task.

To create or modify an SNMP view record, use the following command in global configuration mode:

Command	Purpose
snmp-server view *view-name oid-tree* {**included** | **excluded**}	Creates or modifies a view record.

To remove a view record, use the **no snmp-server view** command.

You can enter this command multiple times for the same view record. Later lines take precedence when an object identifier is included in two or more lines.

Creating or Modifying Access Control for an SNMP Community

Use an SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to permit access to the agent on the router. Optionally, you can specify one or more of the following characteristics associated with the string:

- An access list of IP addresses of the SNMP managers that are permitted to use the community string to gain access to the agent.
- A MIB view, which defines the subset of all MIB objects accessible to the given community.
- Read and write or read-only permission for the MIB objects accessible to the community.

To configure a community string, use the following command in global configuration mode:

Command	Purpose
snmp-server community *string* [**view** *view-name*] [**ro** | **rw**] [*number*]	Defines the community access string.

You can configure one or more community strings. To remove a specific community string, use the **no snmp-server community** command.

For an example of configuring a community string, see the “SNMP Examples” section on page 270.

Specifying an SNMP-Server Engine Name (ID)

To specify an identification name (ID) for either the local or remote SNMP engine on the router, use the following command in global configuration mode:

Command	Purpose
snmp-server engineID [**local** *engineid-string*] | [**remote** *ip-address* **udp-port** *port-number engineid-string*]	Configures names for both the local and remote SNMP engine (or copy of SNMP) on the router.

Specifying SNMP-Server Group Names

To configure a new SNMP group, or a table that maps SNMP users to SNMP views, use the following command in global configuration mode:

Command	Purpose
snmp-server group [*groupname* {**v1** | **v2c** | **v3** [**auth** | **noauth** | **priv**]}][**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]	Configures a new SNMP group, or a table that maps SNMP users to SNMP views.

Configuring SNMP-Server Hosts

To configure the recipient of an SNMP trap operation, use the following command in global configuration mode:

Command	Purpose
snmp-server host *host* [**traps** | **informs**][**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]	Configures the recipient of an SNMP trap operation.

Configuring SNMP-Server Users

To configure a new user to an SNMP group, use the following command in global configuration mode:

Command	Purpose
snmp-server user *username* [*groupname* **remote** *ip-address* [**udp-port** *port*] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password* [**priv des56** *priv password*]] [**access** *access-list*]	Configures a new user to an SNMP group.

Enabling the SNMP Agent Shutdown Mechanism

Using SNMP packets, a network management tool can send messages to users on virtual terminals and the console. This facility operates in a similar fashion to the EXEC **send** command; however, the SNMP request that causes the message to be issued to the users also specifies the action to be taken after the message is delivered. One possible action is a shutdown request. After a system is shut down, typically it is reloaded. Because the ability to cause a reload from the network is a powerful feature, it is protected by the **snmp-server system-shutdown** global configuration command. If you do not issue this command, the shutdown mechanism is not enabled. To enable the SNMP agent shutdown mechanism, use the following command in global configuration mode:

Command	Purpose
snmp-server system-shutdown	Enables system-shutdown using the SNMP message reload feature.

Establishing the Contact, Location, and Serial Number of the SNMP Agent

You can set the system contact, location, and serial number of the SNMP agent so that these descriptions can be accessed through the configuration file. To do so, use one or more of the following commands in global configuration mode:

Command	Purpose
snmp-server contact *text*	Sets the system contact string.
snmp-server location *text*	Sets the system location string.
snmp-server chassis-id *number*	Sets the system serial number.

Defining the Maximum SNMP Agent Packet Size

You can set the maximum packet size permitted when the SNMP agent is receiving a request or generating a reply. To do so, use the following command in global configuration mode:

Command	Purpose
snmp-server packetsize *byte-count*	Establishes the maximum packet size.

Limiting TFTP Servers Used Via SNMP

You can limit the TFTP servers used for saving and loading configuration files via SNMP to the servers specified in an access list. To do so, use the following command in global configuration mode:

Command	Purpose
snmp-server tftp-server-list *number*	Limits TFTP servers used for configuration file copies via SNMP to the servers in an access list.

Monitoring SNMP Status

To monitor SNMP status and information, use the following command in EXEC mode:

Command	Purpose
show snmp	Monitors SNMP status.
show snmp engineID [**local** | **remote**]	Displays information on the local SNMP engine and all remote engines that have been configured on the device.
show snmp groups	Displays information on each SNMP group on the network.
show snmp user	Displays information on each SNMP username in the SNMP users table.

Disabling the SNMP Agent

To disable any version of SNMP, use the following command in global configuration mode:

Command	Purpose
`no snmp-server`	Disables SNMP agent operation.

Configuring SNMP Traps

Note Most Cisco IOS commands use the word "traps" in their command syntax. Unless there is an option within the command to specify either traps or informs, the keyword **traps** should be taken to mean either traps or informs, or both. Use the **snmp-server host** command to specify whether you want SNMP notifications to be sent as traps or informs.
The SNMP Proxy manager must be available and enabled on the device for informs to be used. The SNMP Proxy manager is shipped with PLUS software images only.

To configure the router to send SNMP traps, use the following commands. The second task is optional.

- Configuring the Router to Send Traps
- Changing Trap Operation Values

Configuring the Router to Send Traps

To configure the router to send traps to a host, use the following commands in global configuration mode:

	Command	Purpose
Step 1	**snmp-server engineID remote** *remote-ip-addr remote-engineID*	Specifies the engineID for the remote host.
Step 2	**snmp-server user** *username groupname* **remote** *remote-ip-addr* **v3**	Configures an SNMP user to be associated with the above host. **Note** You cannot configure a remote user for an address without configuring the engineID for that remote host first. This is a restriction imposed in the design of these commands; if you try to configure the user before the host, you will receive a warning message and the command will not be executed.
Step 3	**snmp-server group** [*groupname* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}}] [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]	Configures a group on a remote device.

	Command	Purpose
Step 4	**snmp-server host** *host-addr* **traps** [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**] }] **groupname** [*notification-type*]	Specifies the recipient of the trap message.
Step 5	**snmp-server enable traps** [*notification-type*] [*notification-option*]	Enables the sending of traps or informs, and specifies the type of notifications to be sent. For details on the notfication types available, see the description of this command in the *Cisco IOS Configuration Fundamentals Command Reference*.

The **snmp-server host** command specifies which hosts will receive traps. The **snmp-server enable traps** command globally enables the trap production mechanism for the specified traps.

In order for a host to receive a trap, an **snmp-server host** command must be configured specifying the intended host, and the trap must be enabled globally through the **snmp-server enable traps** command.

Changing Trap Operation Values

Optionally, you can specify a value other than the default for the source interface, message (packet) queue length for each host, or retransmission interval.

To change trap operation values, use any of the following optional commands in global configuration mode:

Command	Purpose
snmp-server trap-source *interface*	Specifies the source interface (and hence IP address) of the trap message. This command also sets the source IP address for informs.
snmp-server queue-length *length*	Establishes the message queue length for each trap host.
snmp-server trap-timeout *seconds*	Defines how often to resend trap messages on the retransmission queue.

Enabling SNMP Informs

To configure the router to send SNMP informs, use the following commands. The second task is optional.

- Configuring the Router to Send Informs
- Changing Inform Operation Values

Configuring the Router to Send Informs

To enable a router to send informs to a host using SNMPv3, perform the following steps:

	Command	Purpose
Step 1	**snmp-server engineID remote** *remote-ip-addr remote-engineID*	Specifies the engineID for the remote host.
Step 2	**snmp-server user** *user-name group-name* **remote** *remote-ip-addr* **v3**	Configures an SNMP user to be associated with the above host. **Note** You cannot configure a remote user for an address without configuring the engineID for that remote host first. This is a restriction imposed in the design of these commands; if you try to configure the user before the host, you will receive a warning message and the command will not be executed.
Step 3	**snmp group** *group-name* **v3 noauth**	Configures a group on a remote device.
Step 4	**snmp-server host** *remote-ip-addr* **informs v3 noauth** *group-name* **config**	Specifies the recipient of the inform message.
Step 5	**snmp-server enable traps** [*notification-type*]	Enables the sending of SNMP notifications (traps or informs).

The **snmp-server host** command specifies which hosts will receive informs. The **snmp-server enable traps** command globally enables the production mechanism for the specified notifications (traps and informs).

In order for a host to receive an inform, an **snmp-server host informs** command must be configured for that host, and the inform must be enabled globally through the use of the **snmp-server enable traps** command.

Changing Inform Operation Values

Optionally, you can specify a value other than the default for number of retries, the retransmission interval, the maximum number of pending requests, or the source IP address.

To change inform operation values, use the following optional command in global configuration mode:

	Command	Purpose
Step 1	**snmp-server informs** [**retries** *retries*] [**timeout** *seconds*] [**pending** *pending*]	Sets options related to resending unacknowledged inform requests.
Step 2	**snmp-server trap-source** *interface*	Specifies the source interface (and hence IP address) of the inform request. This command also changes the source interface for traps.

Configuring the Router as an SNMP Manager

The SNMP manager feature allows a router to act as a network management station. (In other words, configuring a router as an SNMP manager allows it to act as an SNMP client.) As an SNMP manager, the router can send SNMP requests to agents and receive SNMP responses and notifications from agents. When the SNMP manager process is enabled, the router can query other SNMP agents and process incoming SNMP traps.

Security Considerations

Most network security policies assume that routers will be accepting SNMP requests, sending SNMP responses, and sending SNMP notifications.

With the SNMP manager functionality enabled, the router may also be sending SNMP requests, receiving SNMP responses, and receiving SNMP notifications. Your security policy implementation may need to be updated prior to enabling this feature.

SNMP requests are typically sent to UDP port 161. SNMP responses are typically sent from UDP port 161. SNMP notifications are typically sent to UDP port 162.

SNMP Sessions

Sessions are created when the SNMP manager in the router sends SNMP requests, such as inform requests, to a host or receives SNMP notifications from a host. One session is created for each destination host. If there is no further communication between the router and host within the session timeout period, the session will be deleted.

The router tracks statistics, such as the average round-trip time required to reach the host, for each session. Using the statistics for a session, the SNMP manager in the router can set reasonable timeout periods for future requests, such as informs, for that host. If the session is deleted, all statistics are lost. If another session with the same host is later created, the request timeout value for replies will return to the default value.

Sessions consume memory. A reasonable session timeout value should be large enough that regularly used sessions are not prematurely deleted, yet small enough such that irregularly used, or one-shot sessions, are purged expeditiously.

Enabling the SNMP Manager

To enable the SNMP manager process and optionally set the session timeout value, use the following commands in global configuration mode:

	Command	Purpose
Step 1	`snmp-server manager`	Enables the SNMP Manager.
Step 2	`snmp-server manager session-timeout` *seconds*	(Optional) Changes the session timeout value.

Monitoring the SNMP Manager

To monitor the SNMP manager process, use any one of the following commands in EXEC mode:

Command	Purpose
show snmp	Displays global SNMP information.
show snmp sessions [**brief**]	Displays information about current sessions.
show snmp pending	Displays information about current pending requests.

SNMP Examples

The following example enables SNMPv1 and SNMPv2C. The configuration permits any SNMP manager to access all objects with read-only permissions using the community string named "public." This configuration does not cause the router to send any traps.

```
snmp-server community public
```

The following example permits any SNMP to access all objects with read-only permission using the community string named "public." The router will also send ISDN traps to the hosts 192.180.1.111 and 192.180.1.33 using SNMPv1 and to the host 192.180.1.27 using SNMPv2C. The community string "public" is sent with the traps.

```
snmp-server community public
snmp-server enable traps isdn
snmp-server host 192.180.1.27 version 2c public
snmp-server host 192.180.1.111 version 1 public
snmp-server host 192.180.1.33 public
```

The following example allows read-only access for all objects to members of access list 4 that specify the "comaccess" community string. No other SNMP managers have access to any objects. SNMP Authentication Failure traps are sent by SNMPv2C to the host cisco.com using the community string "public."

```
snmp-server community comaccess ro 4
snmp-server enable traps snmp authentication
snmp-server host cisco.com version 2c public
```

The following example sends Entity MIB traps to the host "cisco.com". The community string is restricted. The first line enables the router to send Entity MIB traps in addition to any traps previously enabled. The second line specifies the destination of these traps and overwrites any previous **snmp-server host** commands for the host "cisco.com".

```
snmp-server enable traps entity
snmp-server host cisco.com restricted entity
```

The following example sends the RFC 1157 *authentication failure*, *warmStart*, *linkUp*, and *linkDown* SNMP traps to address 172.30.2.160:

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

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
```

In the following example, the SNMP manager is enabled and the session timeout is set to a larger value than the default:

```
snmp-server manager
snmp-server manager session-timeout 1000
```