CHAPTER 30

Configuring SNMP

This chapter describes how to configure the Simple Network Management Protocol (SNMP) on the Cisco ME 3400E Ethernet Access switch.

Note For complete syntax and usage information for the commands used in this chapter, see the switch command reference for this release *Cisco IOS Commands Master List, Release 12.2* at this URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_product_indices_list.html
For commands for MIB bulk statistics data collection and process MIB configuration, see the *Commands Master List, Release 12.4,* at this URL: http://www.cisco.com/en/US/products/ps6350/products_product_indices_list.html

This chapter consists of these sections:

Understanding SNMP

SNMP is an application-layer protocol that provides a message format for communication between managers and agents. The SNMP system consists of an SNMP manager, an SNMP agent, and a MIB. The SNMP manager can be part of a network management system (NMS) such as CiscoWorks. The agent and MIB reside on the switch. To configure SNMP on the switch, you define the relationship between the manager and the agent.

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 the 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.

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

Although the switch does not support the Cisco Data Collection MIB, you can use the command-line interface to periodically transfer selected MIB data to specified NMS stations. Starting with this release, you can also configure a Cisco Process MIB CPU threshold table.

SNMP Versions

- SNMPv1—The Simple Network Management Protocol, a Full Internet Standard, defined in RFC 1157.

  SNMPv2C replaces the Party-based Administrative and Security Framework of SNMPv2Classic with the community-string-based Administrative Framework of SNMPv2C while retaining the bulk retrieval and improved error handling of SNMPv2Classic. It has these features:

  –
  defined in RFCs 1902 through 1907.
  – SNMPv2C—The community-string-based Administrative Framework for SNMPv2, an Experimental Internet Protocol defined in RFC 1901.

  SNMPv3—Version 3 of the SNMP is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by authenticating and encrypting packets over the network and includes these security features:

  – Message integrity—ensuring that a packet was not tampered with in transit
  – Authentication—determining that the message is from a valid source
  – Encryption—mixing the contents of a package to prevent it from being read by an unauthorized source.

  To select encryption, enter the **priv**

expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes in SNMPv2C report the error type.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy set up for a user and the group within which the user resides. A security level is the permitted level of security within a security model. A combination of the security level and the security model determine which security mechanism is used when handling an SNMP packet. Available security models are SNMPv1, SNMPv2C, and SNMPv3.

Table 30-1 identifies the characteristics of the different combinations of security models and levels.

Table 30-1 SNMP Security Models and Levels

Model	Level	Authentication	Encryption	Result
		MD5 or SHA	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
SNMPv3	authPriv (requires the cryptographic software image)	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.

You must configure the SNMP agent to use the SNMP version supported by the management station. Because an agent can communicate with multiple managers, you can configure the software to support communications using SNMPv1, SNMPv2C, or SNMPv3.

SNMP Manager Functions

Table 30-2 SNMP Operations

Operation	Description
	[1]
get-bulk-request[2]	Retrieves large blocks of data, such as multiple rows in a table, that would otherwise require the transmission of many small blocks of data.
get-response	Replies to a get-request, get-next-request, and set-request sent by an NMS.
set-request	Stores a value in a specific variable.
trap	An unsolicited message sent by an SNMP agent to an SNMP manager when some event has occurred.

1. With this operation, an SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within a table.
2. The **get-bulk** command only works with SNMPv2 or later.

SNMP Agent Functions

- Get a MIB variable—The SNMP agent begins this function in response to a request from the NMS. The agent retrieves the value of the requested MIB variable and responds to the NMS with that value.

  Set a MIB variable—The SNMP agent begins this function in response to a message from the NMS. The SNMP agent changes the value of the MIB variable to the value requested by the NMS.

The SNMP agent also sends unsolicited trap messages to notify an NMS that a significant event has occurred on the agent. Examples of trap conditions include, but are not limited to, when a port or module goes up or down, when spanning-tree topology changes occur, and when authentication failures occur.

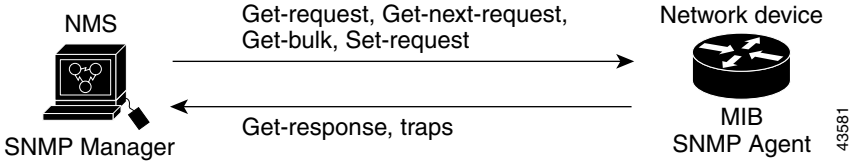
SNMP Community Strings

-
-

Using SNMP to Access MIB Variables

get-request *get-next-request* *set-request*

Figure 30-1 SNMP Network



Appendix A, “Supported MIBs.”

SNMP Notifications

traps

snmp-server host

SNMP ifIndex MIB Object Values

ifIndex Values

Interface Type	ifIndex Range
	1–4999
EtherChannel	5000–5012
Loopback	5013–5077
Tunnel	5078–5142
Physical (such as Gigabit Ethernet or SFP[2]-module interfaces)	10000–14500
Null	14501

SVI = switch virtual interface

2. SFP = small form-factor pluggable

Note

MIB Data Collection and Transfer

bulk-statistics

Configuring SNMP

Default SNMP Configuration

Table 30-4 Default SNMP Configuration

Feature	Default Setting
	tty
	version
	noauth

snmp-server

SNMP Configuration Guidelines

host *engine ID*

associated with that user. Modifying the group's notify view affects all users associated with that group. See the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*

snmp-server engineID **remote**

auth

priv

snmp-server user

Disabling the SNMP Agent

Beginning in privileged EXEC mode, follow these steps to disable the SNMP agent:

	Command	Purpose
Step 1	**configure terminal**	
Step 2	**no snmp-server**	
Step 3	**end**	
Step 4	**show running-config**	
Step 5		

The global configuration command disables all running versions (Version 1, Version 2C, and Version 3) on the device. No specific Cisco IOS command exists to enable SNMP. The first global configuration command that you enter enables all versions of SNMP.

You use the 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 switch. Optionally, you can specify one or more of these 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

[*view-name*] [|] [ ]	Configure the community string. The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command. For , specify a string that acts like a password and permits access to the SNMP protocol. You can configure one or more community strings of any length. (Optional) For , specify the view record accessible to the community. (Optional) Specify either read-only ( ) if you want authorized management stations to retrieve MIB objects, or specify read-write ( ) if you want authorized management stations to retrieve and modify MIB objects. By default, the community string permits read-only access to all objects. (Optional) For , enter an IP standard access list numbered from 1 to 99 and 1300 to 1999.
{ | } [ ]	(Optional) If you specified an IP standard access list number in Step 2, then create the list, repeating the command as many times as necessary. For , enter the access list number specified in Step 2. The keyword denies access if the conditions are matched. The keyword permits access if the conditions are matched. For , enter the IP address of the SNMP managers that are permitted to use the community string to gain access to the agent. (Optional) For , enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore. Recall that the access list is always terminated by an implicit deny statement for everything.
	Return to privileged EXEC mode.
	Verify your entries.

Step 6

```
Switch(config)# snmp-server community comaccess ro 4
```

Configuring SNMP Groups and Users

	Command	Purpose
Step 1		
Step 2		• **engineID local 1234** **remote**

snmp-server group **v1** **v2c** | **v3** **auth** **noauth** **priv** **read** **write** **notify** *notifyview* **access** *access-list*	*groupname,* **v1** **v2c** **v3,** **auth** **noauth** **priv** **priv** **read** **write** **notify** **access**

Command	Purpose
snmp-server user **remote udp-port v1 access v2c access | v3 encrypted access auth md5 sha**	**remote** **v1 v2c v3 v3** **encrypted** **v3** **auth** **md5** **sha** **access**
end	
show running-config	
Step 7 **copy running-config startup-config**	

snmp-server host

Table 30-5 Switch Notification Types

Notification Type Keyword	Description
bgp	
bridge	

Switch Notification Types (continued)

bulkstat collection transfer	
config	
copy-config	
cpu threshold	
entity	
envmon	
ethernet	
flash	
hsrp	
ipmulticast	
mac-notification	
msdp	
ospf	
pim	
port-security	**port-security** **snmp-server enable traps port-security** **snmp-server enable traps port-security trap-rate**
rtr	
snmp	
storm-control	
stpx	
syslog	
tty	
vlan-membership	
vlancreate	
vlandelete	

	Command	Purpose
		snmp-server enable traps ? **snmp-server enable traps** **port-security** **snmp-server enable traps port-security** **snmp-server enable traps port-security trap-rate**
	snmp-server trap-source	
Step 8	**snmp-server queue-length**	
Step 9		
Step 10		
Step 11		
Step 12		

Setting the Agent Contact and Location Information

	Command	Purpose
Step 1		
Step 2		`snmp-server contact Dial System Operator at beeper 21555.`
		`snmp-server location Building 3/Room 222`

Limiting TFTP Servers Used Through SNMP

access-list-number | *source source-wildcard*	*access-list-number* *source* *source-wildcard*

Periodic

MIB Data Collection and Transfer Mechanism

snmp-server mib bulkstat object-list *list-name*	
add *object-name* | *oid*	*object-name,* *oid,*
schema-name	


```
                    snmp mib bulkstat object-list ifMIB
Switch(config-bulk-objects)# add 1.3.6.1.2.1.2.1.2.2.2.1.11
                             add ifName
                             exit
                    snmp mib bulkstat schema testschema
                            object-list ifMIB
                            instance wild oil 1
                            poll-interval 1
                            exit
```

buffer-size	
format bulkBinary bulkASCII schemaASCII	**schemaASCII**
schema	

URL	
number	
minutes	

no enable
enable
enable

```
Switch(config-bulk-tr)# format schemaASCII
                        buffer-size 2147483647
                        schema testschema1
                        schema testschema2
                        transfer-interval 1
                        url primary tftp://host/folder/bulkstat1
                        retain 20
                        retry 2
                        enable
                        exit
```

	Command	Purpose
Step 1		
Step 2		• •
Step 3		• • • •
Step 4		
Step 5		

SNMP Examples

```
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
```

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

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

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

```
snmp-server engineID remote 192.180.1.27 00000063000100a1c0b4011b
snmp-server group authgroup v3 auth
snmp-server user authuser authgroup remote 192.180.1.27 v3 auth md5
mypassword
snmp-server user authuser authgroup v3 auth md5 mypassword
snmp-server host 192.180.1.27 informs version 3 auth authuser config
snmp-server enable traps
snmp-server inform retries 0
```

```
snmp-server enable traps bulkstat
snmp-server host 192.180.1.27 informs version 2 public bulkstat
```

```
snmp-server enable traps cpu threshold
snmp-server host 192.180.1.27 informs version 2 public cpu
```

Displaying SNMP Status

Table 30-6 Commands for Displaying SNMP Information
