



CHAPTER 31

Configuring SNMP

This chapter describes how to configure the Simple Network Management Protocol (SNMP) on the Catalyst 3560 switch.



Note

For complete syntax and usage information for the commands used in this chapter, see the command reference for this release *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2* **Documentation > Cisco IOS Software 12.2 Mainline**

Command References

This chapter consists of these sections:

- [Understanding SNMP, page 31-1](#)
[Configuring SNMP, page 31-6](#)
[Displaying SNMP Status, page 31-18](#)

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.

These sections contain this conceptual information:

- [SNMP Versions, page 31-2](#)
- [SNMP Manager Functions, page 31-3](#)
- [SNMP Agent Functions, page 31-3](#)

- [Using SNMP to Access MIB Variables](#), page 31-4
- [Using SNMP to Access MIB Variables](#), page 31-4
- [SNMP Notifications](#), page 31-5
- [SNMP ifIndex MIB Object Values](#), page 31-5

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 31-1 identifies the characteristics of the different combinations of security models and levels.

Table 31-1 *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 31-2 *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.

SNMP Community Strings

-
-
-

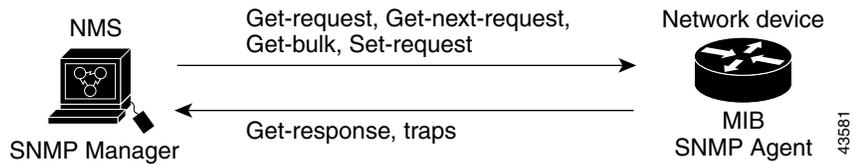
@esN N

Chapter 6, "Clustering Switches" and see *Getting Started with Cisco Network Assistant*

Using SNMP to Access MIB Variables

get-request get-next-request set-request

Figure 31-1 SNMP Network



SNMP Notifications

snmp-server host *traps*



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

Configuring SNMP

-
-
-
-
-
-
-
-
-
-

Default SNMP Configuration

Table 31-4 Default SNMP Configuration

Feature	Default Setting
	tty
	version
	noauth
	snmp-server

SNMP Configuration Guidelines

engine ID

-

associated with that user. Modifying the group's notify view affects all users associated with that group. See the [SNMP notify view configuration](#) for information about when you should configure notify views.

To configure a remote user, specify the IP address or port number for the remote SNMP agent of the device where the user resides.

Before you configure remote users for a particular agent, configure the SNMP engine ID, using the `snmp-server engineID remote` command.

`priv`

`auth`

`snmp-server user`

Disabling the SNMP Agent

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

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

The `snmp-server disable` 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 `snmp-server enable` global configuration command that you enter enables all versions of SNMP.

Configuring Community Strings

-
-
-

Command	Purpose
Step 1	
Step 2 <code>view-name] [] [access-list-number]</code>	<p>Configure the community string.</p> <p>The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.</p> <p>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.</p> <p>(Optional) For , specify the view record accessible to the community.</p> <p>(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.</p> <p>(Optional) For , enter an IP standard access list numbered from 1 to 99 and 1300 to 1999.</p>



	Command	Purpose
Step 3	<pre> } [{ </pre>	<p>(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.</p> <p>For , enter the access list number specified in Step 2.</p> <p>The keyword denies access if the conditions are matched. The keyword permits access if the conditions are matched.</p> <p>For , enter the IP address of the SNMP managers that are permitted to use the community string to gain access to the agent.</p> <p>(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.</p> <p>Recall that the access list is always terminated by an implicit deny statement for everything.</p>
		Return to privileged EXEC mode.
		Verify your entries.
Step 6		



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

Configuring SNMP Groups and Users

	<p style="text-align: center;">snmp-server engineID local 1234</p> <p style="text-align: center;">remote</p>
<p>snmp-server group v1 v2c v3</p> <p>auth noauth priv read</p> <p>write notify notifyview access</p> <p><i>access-list</i></p>	<p><i>groupname,</i></p> <p>v1</p> <p>v2c</p> <p>v3,</p> <p>auth</p> <p>noauth</p> <p>priv</p> <p>priv</p> <p>read</p> <p>write</p> <p>notify</p> <p>access</p>

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



```
host
traps
snmp-server
```

Table 31-5 Switch Notification Types

Notification Type Keyword	Description
bgp	
bridge	
cluster	

Switch Notification Types (continued)

config	
copy-config	
entity	
cpu threshold	
envmon	
errdisable	
flash	
hsrp	
ipmulticast	
mac-notification	
msdp	
ospf	
pim	
port-security	<p>Note port-security</p> <ul style="list-style-type: none"> • snmp-server enable traps port-security • snmp-server enable traps port-security trap-rate
rtr	
snmp	
storm-control	
stp	
syslog	
tty	
vlan-membership	
vlancreate	
vlandelete	
vtp	



fru-ctrl, insertion removal
snmp-server host snmp-server enable traps
 informs

snmp-server host

configure terminal	
snmp-server engineID remote	
snmp-server user remote udp-port v1 access v2c access v3 encrypted access auth md5 sha	
snmp-server group v1 v2c v3 auth noauth priv read write notify access	

Command	Purpose
snmp-server host informs traps version 1 2c 3 auth noauth priv	<p style="text-align: center;">informs</p> <p style="text-align: center;">traps</p> <p style="text-align: center;">version 1 2c 3</p> <p style="text-align: right;">auth, noauth</p> <p>priv</p> <p style="text-align: center;">priv</p> <p style="text-align: center;">version 1 version 2c</p> <p style="text-align: center;">version 3</p>
snmp-server enable traps	<p style="text-align: center;">snmp-server enable traps ?</p> <p style="text-align: right;">snmp-server</p> <p>enable traps</p> <p style="text-align: center;">port-security</p> <p>snmp-server enable traps port-security</p> <p>snmp-server enable traps port-security trap-rate</p>
snmp-server trap-source	
Step 8 snmp-server queue-length	
Step 9	
Step 10	
Step 11	
Step 12	

Setting the CPU Threshold Notification Types and Values

	Command	Purpose
Step 1		
Step 2		<ul style="list-style-type: none"> • • • • • •
Step 3		
Step 4		
Step 5		

Setting the Agent Contact and Location Information

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

Limiting TFTP Servers Used Through SNMP

SNMP Examples

```
snmp-server community public
```

```
snmp-server community public
snmp-server enable traps vtp
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
```

mypassword

```
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
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
```

Displaying SNMP Status

Table 31-6 *Commands for Displaying SNMP Information*
