



Configuring SNMP

This chapter describes how to configure the Simple Network Management Protocol (SNMP) on the Catalyst enterprise LAN switches.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Command Reference* publication for your switch.

This chapter consists of these sections:

- Understanding How SNMP Works, page 25-1
- SNMP Default Configuration, page 25-3
- Configuring SNMP from a NMS, page 25-3
- Configuring SNMP from the CLI, page 25-3
- Using CiscoWorks2000, page 25-5

Understanding How SNMP Works

The components of SNMP network management fall into three categories:

- Managed devices (such as a switch)
- SNMP agents and management information bases (MIBs), including Remote Monitoring (RMON) MIBs, which run on managed devices
- SNMP management applications, such as CiscoWorks2000, which communicate with agents to get statistics and alerts from the managed devices



Note

An SNMP management application, together with the computer it runs on, is called a network management system (NMS).

SNMP network management uses these SNMP agent functions:

- Accessing a MIB variable—This function is initiated by the SNMP agent 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.
- Setting a MIB variable—This function is also initiated by the SNMP agent 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 trap—This function is used to notify an NMS that a significant event has occurred at an agent. When a trap condition occurs, the SNMP agent sends an SNMP trap message to any NMSs specified as the trap receivers, under the following conditions:
 - When a port or module goes up or down
 - When temperature limitations are exceeded
 - When there are spanning-tree topology changes
 - When there are authentication failures
 - When power supply errors occur
- SNMP community strings—SNMP community strings authenticate access to MIB objects and function as embedded passwords:
 - Read-only—Gives read access to all objects in the MIB except the community strings, but does not allow write access
 - Read-write—Gives read and write access to all objects in the MIB, but does not allow access to the community strings
 - Read-write-all—Gives read and write access to all objects in the MIB, including the community strings



Note

The community string definitions on your NMS must match at least one of the three community string definitions on the switch.

The Catalyst enterprise LAN switches are managed devices that support SNMP network management with the following features:

- SNMP traps (see the “Configuring SNMP from the CLI” section on page 25-3)
- RMON in the supervisor engine module software (see Chapter 26, “Configuring RMON”)
- RMON and RMON2 on a Network Analysis Module (see Chapter 28, “Configuring the Network Analysis Module”)
- RMON and RMON2 on an external SwitchProbe device



Note

For more information about MIBs, refer to the *Enterprise MIB User Quick Reference* on Cisco Connection Online (<http://www.cisco.com>).

SNMP ifIndex Persistence Feature

The SNMP ifIndex persistence feature is always enabled. With the ifIndex persistence feature, the ifIndex value of the port and VLAN is always retained and used after the following occurrences:

- Switch reboot
- High-availability switchover
- Software upgrade
- Module reset
- Module removal and insertion of the same type of module

For Fast EtherChannel and Gigabit EtherChannel interfaces, the ifIndex value is only retained and used after a high-availability switchover.

SNMP Default Configuration

Table 25-1 describes the SNMP default configuration.

Table 25-1 SNMP Default Configuration

Feature	Default Setting
SNMP community strings	<ul style="list-style-type: none"> • Read-Only: Public • Read-Write: Private • Read-Write-all: Secret
SNMP trap receiver	None configured
SNMP traps	None enabled

Configuring SNMP from a NMS

To configure SNMP from an Network Management System (NMS), refer to the NMS documentation (see the “Using CiscoWorks2000” section on page 25-5).

The switch supports up to 20 trap receivers through the RMON2 trap destination table. Configure the RMON2 trap destination table from the NMS.

Configuring SNMP from the CLI



Note

This section provides very basic SNMP configuration information. For detailed information on the SNMP commands supported by the Catalyst enterprise LAN switches, refer to the *Command Reference* publication for your switch.

To configure SNMP from the command-line interface (CLI), perform this task in privileged mode:

	Task	Command
Step 1	Define the SNMP community strings for each access type.	set snmp community read-only <i>community_string</i> set snmp community read-write <i>community_string</i> set snmp community read-write-all <i>community_string</i>
Step 2	Assign a trap receiver and community. You can specify up to ten trap receivers.	set snmp trap <i>rcvr_address rcvr_community</i>
Step 3	Specify the SNMP traps to send to the trap receiver.	set snmp trap enable [all module chassis bridge repeater auth vtp ippermit vmpls config entity stpx]
Step 4	Verify the SNMP configuration.	show snmp

This example shows how to define community strings, assign a trap receiver, and specify which traps to send to the trap receiver:

```

Console> (enable) set snmp community read-only Everyone
SNMP read-only community string set to 'Everyone'.
Console> (enable) set snmp community read-write Administrators
SNMP read-write community string set to 'Administrators'.
Console> (enable) set snmp community read-write-all Root
SNMP read-write-all community string set to 'Root'.
Console> (enable) set snmp trap 172.16.10.10 read-write
SNMP trap receiver added.
Console> (enable) set snmp trap 172.16.10.20 read-write-all
SNMP trap receiver added.
Console> (enable) set snmp trap enable all
All SNMP traps enabled.
Console> (enable) show snmp
RMON:                               Disabled
Extended RMON:                       Extended RMON module is not present
Traps Enabled:
Port, Module, Chassis, Bridge, Repeater, Vtp, Auth, ippermit, Vmps, config, entity, stpx
Port Traps Enabled: 1/1-2, 4/1-48, 5/1
Community-Access      Community-String
-----
read-only             Everyone
read-write            Administrators
read-write-all       Root
Trap-Rec-Address      Trap-Rec-Community
-----
172.16.10.10         read-write
172.16.10.20         read-write-all
Console> (enable)

```

**Note**

To disable access for an SNMP community, set the community string for that community to the null string (do not enter a value for the community string).

Using CiscoWorks2000

CiscoWorks2000 is a family of Web-based and management platform-independent products for managing Cisco enterprise networks and devices. CiscoWorks2000 includes Resource Manager Essentials and CWSI Campus, which allow you to deploy, configure, monitor, manage, and troubleshoot a switched internetwork. For more information, see the following publications:

- *Getting Started with Resource Manager Essentials*
- *Getting Started with CWSI Campus*

