



General Switch Administration

This chapter provides these switch administration topics:

- Basic IP connectivity to the switch
- Switch software releases
- Console port access
- Hypertext Transfer Protocol (HTTP) access
- Telnet access
- Simple Network Management Protocol (SNMP) network management platforms
- Default settings of key software features

Refer to the release notes for information about starting up the switch:

- Software and hardware requirements and compatibility
- Browser and Java plug-in configurations
- Setup program

Also refer to the release notes for information about switch software upgrades.

For information about the standard IOS Release 12.1 commands, refer to the IOS documentation set available from the Cisco.com home page at **Service and Support > Technical Documents**. On the Cisco Product Documentation home page, select Release 12.1 from the Cisco IOS Software drop-down list.

Basic IP Connectivity to the Switch

The switch uses IP address information to communicate with the local routers and the Internet. You need this if you plan to use the CMS to configure and manage the switch. The switch also requires a secret password. The IP information is

- Switch IP address
- Subnet mask (IP netmask)
- Default gateway (router)

Once IP information is assigned, you can run the switch with its default settings or configure any settings to meet your network requirements.

The first time that you access the switch, it runs a setup program that prompts you enter this information. For information about running the setup program and assigning basic information to the switch, refer to the release notes.

Switch Software Releases

The switch software is regularly updated with new features and bug fixes, and you might want to upgrade your Catalyst 2950 with the latest software release. New software releases are posted on Cisco.com on the World Wide Web and are available through authorized resellers. Cisco also supplies a TFTP server that you can download from Cisco.com.

Before upgrading a switch, first find out the software version that the switch is running. You can do this by using the Software Upgrade window, by selecting **Help > About**, or by using the **show version** privileged EXEC command.

Knowing the software version is also important for compatibility reasons, especially for switch clusters. Refer to the release notes for this information:

- Compatibility requirements
- Upgrade guidelines and procedures and software reload information

Console Port Access

The switch console port provides switch access to a directly-attached terminal or PC or to a remote terminal or PC through a serial connection and a modem. For information about connecting to the switch console port, refer to the switch hardware installation guide.

Be sure that the switch console port settings match the settings of the terminal or PC. These are the default settings of the switch console port:

- Baud rate default is 9600.
- Data bits default is 8.



Note If the data bits option is set to 8, set the parity option to None.

- Stop bits default is 1.
- Parity settings default is None.

Make sure that you save any changes that you make to the switch console port settings to Flash memory. For information about saving changes from CMS, see the [“Saving Your Changes” section on page 2-32](#). For information about saving changes from the CLI, see the [“Saving Configuration Changes” section on page 3-10](#).

Telnet Access to the CLI

This procedure assumes that you have assigned IP information and a Telnet password to the switch or the command switch, as described in the release notes. Information about accessing the CLI through a Telnet session is in the [“Accessing the CLI” section on page 3-9](#).

To configure the switch for Telnet access, follow these steps:

	Command	Purpose
Step 1		Attach a PC or workstation with emulation software to the switch console port. The default data characteristics of the switch console port are 9600, 8, 1, no parity. When the command line appears, go to Step 2.
Step 2	enable	Enter privileged EXEC mode.
Step 3	config terminal	Enter global configuration mode.
Step 4	line vty 0 15	Enter the interface configuration mode for the Telnet interface. There are 16 possible sessions on a command-capable switch. The 0 and 15 mean that you are configuring all 16 possible Telnet sessions.
Step 5	password <i><password></i>	Enter an enable secret password.
Step 6	end	Return to privileged EXEC mode so that you can verify the entry.
Step 7	show running-config	Display the running configuration. The password is listed under the command line vty 0 15
Step 8	copy running-config startup-config	(Optional) Save the running configuration to the startup configuration.

HTTP Access to CMS

CMS uses Hypertext Transfer Protocol (HTTP), which is an in-band form of communication with the switch through any one of its Ethernet ports and that allows switch management from a standard web browser. The default HTTP port is 80.

If you change the HTTP port, you must include the new port number when you enter the IP address in the browser Location or Address field (for example, <http://10.1.126.45:184> where 184 is the new HTTP port number).



Note

The HTTP Port option on CMS is not available if your access level to the switch is read-only. For more information about the read-only access mode, see the [“Access Modes in CMS” section on page 2-31](#).

Do not disable or otherwise misconfigure the port through which your management station is communicating with the switch. You might want to write down the port number to which your station is connected. Make changes to the switch IP information with care.



Note

The HTTP Port option on CMS is not available if your access level to the switch is read-only. For more information about the read-only access mode see the [“Access Modes in CMS” section on page 2-31](#).

Refer to these topics in the release notes for information about accessing CMS:

- System requirements
- Running the setup program, which includes assigning a privilege-level 15 password for accessing CMS
- Installing the required Java plug-in

- Configuring your web browser
- Displaying the Cisco Systems Access page

You can also see the [“Accessing CMS” section on page 2-30](#).

For information about connecting to a switch port, refer to the switch hardware installation guide.

SNMP Network Management Platforms

You can manage switches by using an Simple Network Management Protocol (SNMP)-compatible management station running such platforms as HP OpenView or SunNet Manager. CiscoWorks2000 and CiscoView 5.0 are network-management applications that you can use to configure, monitor, and troubleshoot Catalyst 2950 switches.

The switch supports a comprehensive set of Management Information Base (MIB) extensions and MIB II, the IEEE 802.1D bridge MIB, and four Remote Monitoring (RMON) groups, which this IOS software release supports. You can configure these groups by using an SNMP application or by using the CLI. The four supported groups are alarms, events, history, and statistics.

This section describes how to access MIB objects to configure and manage your switch. It provides this information:

- Using File Transfer Protocol (FTP) to access the MIB files
- Using SNMP to access the MIB variables

In a cluster configuration, the command switch manages communication between the SNMP management station and all switches in the cluster. For information about managing cluster switches through SNMP, see the [“Using SNMP to Manage Switch Clusters” section on page 5-24](#).

When configuring your switch by using SNMP, note that certain combinations of port features create configuration conflicts. For more information, see the [“Avoiding Configuration Conflicts” section on page 14-1](#).

SNMP Versions

This software release supports these SNMP versions:

- SNMPv1—The Simple Network Management Protocol, a Full Internet Standard, defined in RFC 1157.
- SNMPv2C, which has these features:
 - SNMPv2—Version 2 of the Simple Network Management Protocol, a Draft Internet Standard, defined in RFCs 1902 through 1907.
 - SNMPv2C—The Community-based Administrative Framework for SNMPv2, an Experimental Internet Protocol defined in RFC 1901.

SNMPv2C replaces the Party-based Administrative and Security Framework of SNMPv2Classic with the Community-based Administrative Framework of SNMPv2C while retaining the bulk retrieval and improved error handling of SNMPv2Classic.

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 includes a bulk retrieval mechanism and more detailed error message reporting to management stations.

The bulk retrieval mechanism retrieves tables and large quantities of information, minimizing the number of round-trips required. The SNMPv2C improved error-handling 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.

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 software to support communications with one management station using the SNMPv1 protocol and another using the SNMPv2 protocol.

Using FTP to Access the MIB Files

You can obtain each MIB file with this procedure:

-
- Step 1** Use FTP to access the server **ftp.cisco.com**.
 - Step 2** Log in with the username *anonymous*.
 - Step 3** Enter your e-mail username when prompted for the password.
 - Step 4** At the `ftp>` prompt, change directories to `/pub/mibs/supportlists`.
 - Step 5** Change directories to this:
 - **wsc2950** for a list of Catalyst 2950 MIBs
 - Step 6** Use the `get MIB_filename` command to obtain a copy of the MIB file.
-

You can also access this server from your browser by entering this URL in the **Location** field of your Netscape browser (the **Address** field in Internet Explorer):

```
ftp://ftp.cisco.com
```

Use the mouse to navigate to the folders listed above.

Using SNMP to Access MIB Variables

The switch MIB variables are accessible through SNMP, an application-layer protocol facilitating the exchange of management information between network devices. The SNMP system consists of these parts:

- The SNMP manager, which resides on the network management system (NMS)
- The SNMP agent, which resides on the switch
- The MIBs that reside on the switch but that can be compiled with your network management software

An example of an NMS is the CiscoWorks network management software. CiscoWorks2000 software uses the switch MIB variables to set device variables and to poll devices on the network for specific information. The results of a poll can be displayed as a graph and analyzed to troubleshoot internetworking problems, to increase network performance, to verify the configuration of devices, to monitor traffic loads, and more.

As shown in [Figure 4-1](#), the SNMP agent gathers data from the MIB, which is the repository for information about device parameters and network data. The agent can send traps, or notification of certain events, to the SNMP manager, which receives and processes the traps. Traps are messages alerting the SNMP manager to a condition on the network such as improper user authentication, restarts, link status (up or down), and so forth. In addition, the SNMP agent responds to MIB-related queries sent by the SNMP manager in *get-request*, *get-next-request*, and *set-request* format.

The SNMP manager uses information in the MIB to perform the operations described in [Table 4-1](#).

Figure 4-1 SNMP Network

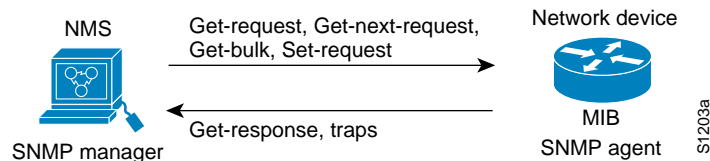


Table 4-1 SNMP Operations

Operation	Description
get-request	Retrieves a value from a specific variable.
get-next-request	Retrieves a value from a variable within a table. ¹
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 about some event that 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.

Default Settings

The switch is designed for plug-and-play operation, requiring only that you assign basic IP information to the switch and connect it to the other devices in your network. For information about assigning basic IP information to the switch, see the [“Basic IP Connectivity to the Switch”](#) section on [page 4-1](#) and the release notes.

If you have specific network needs, you can configure the switch through its various management interfaces. [Table 4-2](#) lists the key software features, their defaults, their page numbers in this guide, and where you can configure them from the command-line interface (CLI) and Cluster Management Suite (CMS).

Table 4-2 Default Settings and Where To Change Them

Feature	Default Setting	Concepts and CLI Procedures	CMS Option
Cluster Management			
Enabling a Command Switch ¹	None	<p>“Enabling a Command Switch” section on page 5-17.</p> <p>No CLI procedure provided. For the cluster commands, refer to the <i>Catalyst 2950 Desktop Switch Command Reference</i>.</p>	<p>Device Manager (not within a cluster session) from a command-capable switch</p> <p>Cluster > Create Cluster</p>
Creating a cluster ¹	None	<p>“Creating a Switch Cluster” section on page 5-16.</p> <p>No CLI procedure. For the cluster commands, refer to the <i>Catalyst 2950 Desktop Switch Command Reference</i>.</p>	<p>Device Manager (not within a cluster session) from a command-capable switch</p> <p>Cluster > Create Cluster</p>
Adding and removing cluster members ²	None	<p>“Adding Member Switches” section on page 5-18.</p> <p>No CLI procedure. For the cluster commands, refer to the <i>Catalyst 2950 Desktop Switch Command Reference</i>.</p>	<p>Cluster > Add to Cluster and</p> <p>Cluster > Remove from Cluster</p>
Creating a standby command-switch group ²	None	<p>“Creating a Cluster Standby Group” section on page 5-20.</p> <p>No CLI procedure. For the cluster commands, refer to the <i>Catalyst 2950 Desktop Switch Command Reference</i>.</p>	<p>Cluster > Standby Commanders</p>
Upgrading cluster software	Enabled	<p>“Switch Software Releases” section on page 4-2.</p> <p>Release notes on Cisco.com.</p>	<p>Administration > Software Upgrade</p>
Configuring SNMP community strings and trap managers	None	<p>“SNMP Community Strings” section on page 5-14 and “Configuring SNMP” section on page 6-12.</p>	<p>Administration > SNMP</p>
Device Management			
Switch IP address, subnet mask, and default gateway	0.0.0.0	<p>“Changing IP Information” section on page 6-1.</p> <p>Documentation set for Cisco IOS Release 12.1 on Cisco.com.</p>	<p>Administration > IP Addresses</p>
Dynamic Host Configuration Protocol (DHCP)	DHCP client is enabled	<p>“Using DHCP-Based Autoconfiguration” section on page 6-2.</p> <p>Documentation set for Cisco IOS Release 12.1 on Cisco.com.</p>	–
HTTP Port	80	<p>“HTTP Access to CMS” section on page 4-3.</p>	<p>Administration > HTTP Port</p>
Management VLAN	VLAN 1	<p>“Management VLANs” section on page 8-3.</p>	<p>VLAN > Management VLAN</p>

Table 4-2 Default Settings and Where To Change Them (continued)

Feature	Default Setting	Concepts and CLI Procedures	CMS Option
Domain name	None	“Configuring the Domain Name and the DNS” section on page 6-5. Documentation set for Cisco IOS Release 12.1 on Cisco.com.	Administration > IP Addresses
Cisco Discovery Protocol (CDP)	Enabled	“Configuring CDP” section on page 6-13. Documentation set for Cisco IOS Release 12.1 on Cisco.com.	Cluster > Hop Count
Address Resolution Protocol (ARP)	Enabled	“Managing the ARP Table” section on page 6-14. Documentation set for Cisco IOS Release 12.1 on Cisco.com.	Administration > ARP
CoS and WRR	Disabled	“CoS and WRR” section on page 13-8.	Device > QoS
System Time Management	None	“Setting the System Date and Time” section on page 6-11. Documentation set for Cisco IOS Release 12.1 on Cisco.com.	Administration > System Time
Mac Address Notification	Disabled	“MAC Address Notification” section on page 6-17.	–
Static address assignment	None assigned	“Adding and Removing Static Address Entries” section on page 6-18. Documentation set for Cisco IOS Release 12.1 on Cisco.com.	Administration > MAC Addresses
Dynamic address management	Enabled	“Managing the MAC Address Tables” section on page 6-15. Documentation set for Cisco IOS Release 12.1 on Cisco.com.	Administration > MAC Addresses
VLAN membership	–	“Assigning VLAN Port Membership Modes” section on page 8-4.	VLAN > VLAN
VMPS Configuration	–	“How the VMPS Works” section on page 8-28.	VLAN > VMPS
VTP Management	VTP server mode	“Configuring VTP” section on page 8-12.	VLAN > VLAN

Table 4-2 Default Settings and Where To Change Them (continued)

Feature	Default Setting	Concepts and CLI Procedures	CMS Option
Performance			
Configuring a port	None	Chapter 10, “Configuring the Switch Ports.”	Port > Port Settings
Duplex mode	Auto	“Changing the Port Speed and Duplex Mode” section on page 10-1.	Port > Port Settings
Speed on 10/100 ports	Auto	“Changing the Port Speed and Duplex Mode” section on page 10-1.	Port > Port Settings
Gigabit Ethernet Flow		“Configuring Flooding Controls” section on page 10-4.	Port > Port Settings
Flooding Control			
Storm control	Disabled	“Configuring Flooding Controls” section on page 10-4.	Port > Flooding Control
Flooding unknown unicast and multicast packets	Enabled	“Configuring Protected Ports” section on page 10-5.	Port > Flooding Control
IGMP Snooping	Enabled	“Understanding and Configuring IGMP Snooping” section on page 11-1. “Enabling or Disabling IGMP Snooping” section on page 11-2. “Immediate-Leave Processing” section on page 11-3. “CLI: Configuring a Multicast Router Port” section on page 11-7.	Device > IGMP Snooping
Multicast VLAN Registration (MVR)	Disabled	“Understanding Multicast VLAN Registration” section on page 11-7.	–
Network Redundancy			
Hot Standby Router Protocol	Disabled	“Creating a Cluster Standby Group” section on page 5-20.	Cluster > Standby Command Switches
Spanning Tree Protocol	Enabled	“Configuring Basic STP Features” section on page 9-20. “Configuring Advanced STP Features” section on page 9-30.	Device > Spanning Tree Protocol (STP)
Unidirectional link detection	Disabled	“Configuring UniDirectional Link Detection” section on page 10-18.	–
Port grouping	None assigned	“Understanding the EtherChannel” section on page 10-8.	Port > EtherChannels
QoS and Security			
Access Control Lists (ACLs) ³	None assigned	“Guidelines for Configuring ACLs on the Catalyst 2950 Switches” section on page 12-5. “Creating Standard and Extended IP ACLs” section on page 12-7.	Device > ACLs

Table 4-2 Default Settings and Where To Change Them (continued)

Feature	Default Setting	Concepts and CLI Procedures	CMS Option
Quality of Service (QoS) ³	Disabled	“Configuring Classification Using Port Trust States” section on page 13-10. “Configuring a QoS Policy” section on page 13-13. “Configuring CoS Maps” section on page 13-21.	Device > QoS
Diagnostics			
Displaying graphs and statistics	Enabled	–	Reports
Switch Port Analyzer (SPAN) port monitoring	Disabled	“Configuring SPAN” section on page 10-22.	Port > Switch Port Analyzer (SPAN)
Console, buffer, and file logging	Disabled	– Documentation set for Cisco IOS Release 12.1 on Cisco.com.	–
Remote monitoring (RMON)	Disabled	“SNMP Network Management Platforms” section on page 4-4. Documentation set for Cisco IOS Release 12.1 on Cisco.com.	–
System Messages		Appendix B, “System Messages.”	Report > System Messages
Security			
Password	None	“Passwords” section on page 5-14 and “Changing the Password” section on page 6-10.	–
Addressing security	Disabled	“Managing the MAC Address Tables” section on page 6-15.	Administration > MAC Addresses
Trap manager	0.0.0.0	“Adding Trap Managers” section on page 6-12.	Administration > SNMP
Community strings	public	“SNMP Community Strings” section on page 5-14 and “Entering Community Strings” section on page 6-12. Documentation set for Cisco IOS Release 12.1 on Cisco.com.	Administration > SNMP
Port security	Disabled	“Enabling Port Security” section on page 10-6.	Port > Port Security
Terminal Access Controller Access Control System Plus (TACACS+)	Disabled	“Configuring TACACS+” section on page 6-20.	–
Protected port	Disabled	“Configuring Protected Ports” section on page 10-5.	Port > Protected Port

Table 4-2 *Default Settings and Where To Change Them (continued)*

Feature	Default Setting	Concepts and CLI Procedures	CMS Option
802.1X port-based authentication	Disabled	“Configuring 802.1X Authentication” section on page 7-6.	Device > 802.1X

1. Available only from a Device Manager session on a command-capable switch that is not a cluster member.
2. Available only from a cluster management session.
3. Available only on a switch running the enhanced software image.

