



General Switch Administration

This chapter provides these switch administration topics:

- [Basic IP Connectivity to the Switch, page 4-2](#)
- [Switch Software Releases, page 4-2](#)
- [Console Port Access, page 4-3](#)
- [Telnet Access to the CLI, page 4-4](#)
- [HTTP Access to CMS, page 4-5](#)
- [SNMP Network Management Platforms, page 4-5](#)
- [Default Settings, page 4-8](#)

The following information tends to change and therefore appear only in the release notes. Before installing, configuring, or upgrading the switch, refer to the release notes (<http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm>) for the latest information about:

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

This switch software release is based on Cisco IOS Release 12.0. It has been enhanced to support a set of features for the Catalyst 2900 XL and Catalyst 3500 XL switches. This chapter provides procedures for using only the commands that have been created or changed for these switches. The *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference* provides complete descriptions of these commands. This chapter does not provide Cisco IOS Release 12.0 commands and information already documented in the Cisco IOS Release 12.0 documentation on Cisco.com.

Basic IP Connectivity to the Switch

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

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

The first time that you access the switch, it runs a setup program that prompts you to assign basic information (such as IP address and passwords) to the switch. For information about running the setup program, refer to the latest switch release notes (<http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm>).

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

For more information about IP information, see the “[Changing IP Information](#)” section on page 6-2. For more information about passwords, see the “[Accessing CMS](#)” section on page 2-32 and “[Assigning Passwords and Privilege Levels](#)” section on page 6-11.

Switch Software Releases

The switch software is regularly updated with new features and bug fixes, and you might want to upgrade your Catalyst 2900 XL and Catalyst 3500 XL 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 version of the software 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** command.

Knowing the software version is also important for compatibility reasons, especially for switch clusters. Refer to the latest switch release notes (<http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm>) 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 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 2-34](#). For information about saving changes from the CLI, see the [“Saving Configuration Changes” section on page 3-8](#).

Telnet Access to the CLI

This procedure assumes that you have assigned IP information and a Telnet password to the switch or command switch, as described in the latest switch release notes (<http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm>). Information about accessing the CLI through a Telnet session is provided in the “Accessing the CLI” section on page 3-7.

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 a enable secret password. For more information about passwords, see the “Assigning Passwords and Privilege Levels” section on page 6-11.
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).

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 you are connected. Changes to the switch IP information should be done with care.

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 you can use to configure, monitor, and troubleshoot Catalyst 2900 XL and Catalyst 3500 XL 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

For more information about SNMP, see the [“Configuring SNMP” section on page 6-48](#).

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 5-25](#).

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 9-2](#).

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 one of the following:
 - **wsc2900xl** for a list of Catalyst 2900 XL MIBs
 - **wsc3500xl** for a list of Catalyst 3500 XL 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 three 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, increase network performance, verify the configuration of devices, 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*

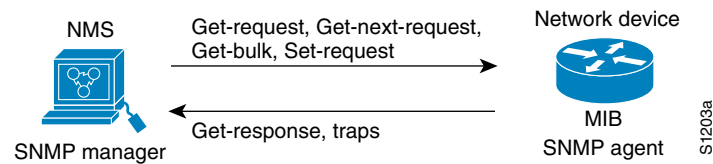


Table 4-1 *SNMP Operations*

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-bulk-request ²	Retrieves large blocks of data, such as multiple rows in a table, which 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 indicating that 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 SNMP version 2.

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 4-2 and the latest switch release notes (<http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm>).

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 5-18.</p> <p>No CLI procedure provided. For the cluster commands, refer to the <i>Catalyst 2900 Series XL and Catalyst 3500 Series XL 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 5-17.</p> <p>No CLI procedure provided. For the cluster commands, refer to the <i>Catalyst 2900 Series XL and Catalyst 3500 Series XL 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 5-19.</p> <p>No CLI procedure provided. For the cluster commands, refer to the <i>Catalyst 2900 Series XL and Catalyst 3500 Series XL 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 5-21.</p> <p>No CLI procedure provided. For the cluster commands, refer to the <i>Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference</i>.</p>	Cluster > Standby Command Switches
Upgrading cluster software	Enabled	<p>“Switch Software Releases” section on page 4-2.</p> <p>Refer to the latest switch release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm).</p>	Administration > Software Upgrade
Configuring SNMP community strings and trap managers	None	<p>“SNMP Community Strings” section on page 5-14 and “Configuring SNMP” section on page 6-48.</p>	Administration > SNMP

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

Feature	Default Setting	Concepts and CLI Procedures	CMS Option
Device Management			
Switch IP address, subnet mask, and default gateway	0.0.0.0	<p>“Changing IP Information” section on page 6-2.</p> <p>Refer to the latest switch release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm).</p> <p>Documentation set for Cisco IOS Release 12.0 on Cisco.com.</p>	Administration > IP Addresses
Dynamic Host Configuration Protocol (DHCP)	DHCP client is enabled	<p>“Using DHCP-Based Autoconfiguration” section on page 6-3.</p> <p>Documentation set for Cisco IOS Release 12.0 on Cisco.com.</p>	–
Domain name	None	<p>“Configuring the Domain Name and the DNS” section on page 6-6.</p> <p>Documentation set for Cisco IOS Release 12.0 on Cisco.com.</p>	Administration > IP Addresses
Cisco Discovery Protocol (CDP)	Enabled	<p>“Configuring CDP” section on page 6-13.</p> <p>Documentation set for Cisco IOS Release 12.0 on Cisco.com.</p>	Cluster > Hop Count
Address Resolution Protocol (ARP)	Enabled	<p>“Managing the ARP Table” section on page 6-32.</p> <p>Documentation set for Cisco IOS Release 12.0 on Cisco.com.</p>	Administration > ARP
System Time Management	None	<p>“Setting the System Date and Time” section on page 6-12.</p> <p>Documentation set for Cisco IOS Release 12.0 on Cisco.com.</p>	Administration > System Time
MAC address notification	Disabled	<p>“MAC Address Notification” section on page 6-17.</p>	–
Static address assignment	None assigned	<p>“Adding Static Addresses” section on page 6-19.</p> <p>Documentation set for Cisco IOS Release 12.0 on Cisco.com.</p>	Administration > MAC Addresses
Dynamic address management	Enabled	<p>“Managing the MAC Address Tables” section on page 6-15.</p> <p>Documentation set for Cisco IOS Release 12.0 on Cisco.com.</p>	Administration > MAC Addresses

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

Feature	Default Setting	Concepts and CLI Procedures	CMS Option
Management VLAN	VLAN 1	“Management VLANs” section on page 8-3.	VLAN > Management VLAN
VLAN membership	Static-access ports in VLAN 1	“Assigning VLAN Port Membership Modes” section on page 8-5.	VLAN > VLAN
VMPS Configuration	–	“How the VMPS Works” section on page 8-35.	VLAN > VMPS
VTP Management	VTP server mode	“Configuring VTP” section on page 8-15.	VLAN > VLAN
Voice VLAN (VVID) configuration	–	“Configuring Voice Ports” section on page 7-14.	VLAN > Voice VLAN
Performance			
Configuring a port	None	Chapter 7, “Configuring the Switch Ports.”	Port > Port Settings
Duplex mode	Auto on all 10/100 ports	“Changing the Port Speed and Duplex Mode” section on page 7-2.	Port > Port Settings
Speed on 10/100 ports	Auto	“Changing the Port Speed and Duplex Mode” section on page 7-2.	Port > Port Settings
Gigabit Ethernet flow control	Asymmetric Note This option is configurable only on the Gigabit ports.	“Configuring Flow Control on Gigabit Ethernet Ports” section on page 7-3.	Port > Port Settings
Inline power	Auto	“Configuring Inline Power on the Catalyst 3524-PWR Ports” section on page 7-17.	–

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

Feature	Default Setting	Concepts and CLI Procedures	CMS Option
Flooding Control			
Storm control	Disabled	“Configuring Flooding Controls” section on page 7-4.	Port > Flooding Control
Flooding unknown unicast and multicast packets	Enabled	“Blocking Flooded Traffic on a Port” section on page 7-5.	Port > Flooding Control
Cisco Group Management Protocol (CGMP)	Enabled	“Configuring CGMP” section on page 6-20.	Device > CGMP
Multicast VLAN Registration (MVR)	Disabled	“Configuring MVR” section on page 6-27.	–
Internet Group Management Protocol (IGMP) filtering	Disabled	“Configuring IGMP Filtering” section on page 6-23.	–
Network Port	Disabled	“Enabling a Network Port” section on page 7-6.	–
Network Redundancy			
Hot Standby Router Protocol	Disabled	“Creating a Cluster Standby Group” section on page 5-21.	Cluster > Standby Command Switches²
Spanning Tree Protocol	Enabled	“Configuring STP” section on page 6-33.	Device > STP
Unidirectional link detection	Disabled	“Configuring UniDirectional Link Detection” section on page 7-7.	–
Port grouping	None assigned	“Creating EtherChannel Port Groups” section on page 7-8.	Port > EtherChannels
Diagnostics			
Displaying statistics, graphs, and reports	Enabled	“Verifying a Switch Cluster” section on page 5-23.	Reports
Switch Port Analyzer (SPAN) port monitoring	Disabled	“Enabling SPAN” section on page 7-13.	Port > SPAN
Console, buffer, and file logging	Disabled	– Documentation set for Cisco IOS Release 12.0 on Cisco.com.	–
Remote monitoring (RMON)	Disabled	“SNMP Network Management Platforms” section on page 4-5. Documentation set for Cisco IOS Release 12.0 on Cisco.com.	–

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

Feature	Default Setting	Concepts and CLI Procedures	CMS Option
Security			
Password	None	<p>“Passwords” section on page 5-14 and “Assigning Passwords and Privilege Levels” section on page 6-11.</p> <p>Refer to the latest switch release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm).</p>	—
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 6-49.	Administration > SNMP
Community strings	public	<p>“SNMP Community Strings” section on page 5-14 and “Entering Community Strings” section on page 6-49.</p> <p>Documentation set for Cisco IOS Release 12.0 on Cisco.com.</p>	Administration > SNMP
Port security	Disabled	“Enabling Port Security” section on page 7-11.	Port > Port Security
Protected port	Disabled	“Configuring Protected Ports” section on page 7-10.	Port > Protected Port
Terminal Access Controller Access Control System Plus (TACACS+)	Disabled	“Configuring TACACS+” section on page 6-51.	—

1. Available only from a Device Manager session on a command-capable switch, which is not a cluster member.
2. Available only from a cluster management session.