



General Switch Administration

This chapter provides these switch administration topics:

- [Initial Switch Configuration, 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 4-3](#)
- [SNMP Network Management Platforms, page 4-4](#)
- [Default Settings, page 4-7](#)

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 switch 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.

Initial Switch Configuration

Initial switch configuration involves these tasks:

- Cabling the switch to a network management station, as described in the switch hardware installation guide.
- Using the setup program to configure basic IP connectivity and access to the switch. The setup program needs this switch information:
 - IP address. The switch uses IP address information to communicate with the local routers and the Internet. You also need a switch IP address if you plan to use CMS to configure and manage the switch.
 - Subnet mask (IP netmask)
 - Default gateway (router)
 - Password

If you plan to use the switch in a switch cluster, the setup program also prompts for the name and password of the cluster.

Complete information about the setup program is in the release notes (<http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm>).

- (For CMS users) Downloading the correct browser plug-in and configuring your Netscape or Internet Explorer browser. Complete information about the browser and plug-in requirements and procedures are in the release notes (<http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm>).

After you have assigned IP information to the switch, you can run the switch on its default settings (Table 4-2) 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 or Catalyst 3500 XL switch with the latest software release. New software releases are posted on Cisco.com 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 selecting **Reports > Inventory**, or by using the **show version** user EXEC command.

Knowing the software version is important, especially for:

- Compatibility reasons (for example, for switch clusters)
- LRE and non-LRE Catalyst 2900 XL switches, which do not share the same software image. The LRE-only image cannot be installed on non-LRE switches. The non-LRE image does not include LRE functionality and therefore should not be installed on LRE switches.

Refer to the release notes (<http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm>) for

- Switch requirements
- Switch upgrade guidelines and procedures

In addition, Catalyst LRE switches can store and properly apply LRE binaries in case there are updates required to the firmware on the switch's local LRE controllers or connected customer premises equipment (CPE) devices. For more information on this feature, see [Upgrading LRE Switch Firmware, page 8-15](#).

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 3-9](#).

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.

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 3-8.

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 <password> | 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. |

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 FTP to Access the MIB Files” section on page 4-5
- “Using SNMP to Access MIB Variables” section on page 4-5

For more information about SNMP, see the “Configuring SNMP” section on page 6-47.

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 5-27.

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 10-7](#).

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*

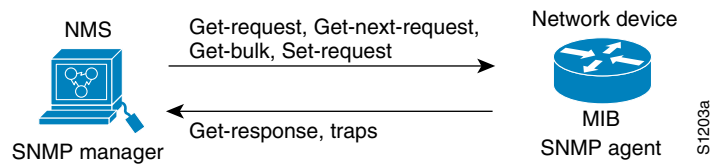


Table 4-1 *SNMP Operations*

| 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 “Initial Switch Configuration” 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 CLI and 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 | “Enabling a Command Switch” section on page 5-20. No CLI procedure provided. For the cluster commands, refer to the switch command reference. | Device Manager (not within a cluster session) from a command-capable switch Cluster > Create Cluster |
| Creating a cluster ¹ | None | “Creating a Switch Cluster” section on page 5-19. No CLI procedure provided. For the cluster commands, refer to the switch command reference. | Device Manager (not within a cluster session) from a command-capable switch Cluster > Create Cluster |
| Adding and removing cluster members ² | None | “Adding Member Switches” section on page 5-21. No CLI procedure provided. For the cluster commands, refer to the switch command reference. | Cluster > Add to Cluster and Cluster > Remove from Cluster |
| Creating a standby command switch group ² | None | “Creating a Cluster Standby Group” section on page 5-23. No CLI procedure provided. For the cluster commands, refer to the switch command reference. | Cluster > Standby Command Switches |
| Upgrading cluster software | Enabled | “Switch Software Releases” section on page 4-2. Refer to the latest switch release notes (http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/index.htm). | Administration > Software Upgrade |
| Configuring SNMP community strings and trap managers | None | “SNMP Community Strings” section on page 5-16 and “Configuring SNMP” section on page 6-47. | 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 6-31.</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 9-3. | VLAN > Management VLAN |
| VLAN membership | Static-access ports in VLAN 1 | “Assigning VLAN Port Membership Modes” section on page 9-5. | VLAN > VLAN |
| VMPS Configuration | – | “How the VMPS Works” section on page 9-36. | VLAN > VMPS |
| VTP Management | VTP server mode | “Using VTP” section on page 9-9. | VLAN > VLAN |
| Voice VLAN (VVID) configuration | – | “Configuring Voice Ports” section on page 7-14. | VLAN > Voice VLAN |
| Performance | | | |
| Configuring ports | – | “Configuring the Switch Ports” section on page 7-1 and “Configuring LRE Ports” section on page 8-6 (for LRE ports only). Note You cannot disable the Cisco 585 LRE CPE Ethernet ports on a per-port basis. You can either enable or disable all Ethernet ports on the CPE device. This restriction does not apply to the Cisco 575 LRE CPE, which has only one Ethernet port. | Port > Port Settings and Device > LRE Profiles (for LRE ports only) |
| Duplex mode | – | “Changing the Port Speed and Duplex Mode” section on page 7-2. <ul style="list-style-type: none"> • Auto on the 10/100, 100BASE-FX, and Gigabit ports • Half duplex on the CPE Ethernet ports Note This option is configurable on the Cisco 575 LRE CPE. It is not configurable on the Cisco 585 LRE CPE. | Port > Port Settings |
| Speed on switch 10/100 and CPE Ethernet ports | Auto | “Changing the Port Speed and Duplex Mode” section on page 7-2. Note This option is configurable on the Cisco 575 LRE CPE. It is not configurable on the Cisco 585 LRE CPE. | Port > Port Settings |
| Gigabit Ethernet flow control | – | “Configuring Flow Control on Gigabit Ethernet Ports” section on page 7-4. <ul style="list-style-type: none"> • Asymmetric on all Gigabit ports • Disabled on LRE ports in half-duplex mode; enabled on LRE ports in full-duplex mode Note This option is configurable only on the Gigabit ports. | Port > Port Settings |
| LRE link speed and LRE port profiles | LRE-10 | “Configuring LRE Ports” section on page 8-6. | Device > LRE Profiles |
| LRE rate selection | enabled | “Using Rate Selection to Automatically Assign Profiles” section on page 8-10 | Device > LRE Rate Selection |
| LRE upgrade | system-wide | “Upgrading LRE Switch Firmware” section on page 8-15 | Administration > LRE Upgrade |
| LRE link persistence | disabled | “LRE Link Persistence” section on page 8-15 | – |

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

| Feature | Default Setting | Concepts and CLI Procedures | CMS Option |
|---|-----------------|--|--|
| Inline power | Auto | “Configuring Inline Power on the Catalyst 3524-PWR Ports” section on page 7-16. | – |
| 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 6-26. | – |
| Internet Group Management Protocol (IGMP) filtering | Disabled | “Configuring IGMP Filtering” section on page 6-22. | – |
| Network Port | Disabled | “Enabling a Network Port” section on page 7-6. | – |
| Network Redundancy | | | |
| Hot Standby Router Protocol ² | Disabled | “Creating a Cluster Standby Group” section on page 5-23. | Cluster > Standby Command Switches |
| Spanning Tree Protocol | Enabled | “Configuring STP” section on page 6-31. | Device > STP |
| Unidirectional link detection (UDLD) | Disabled | “Configuring UniDirectional Link Detection” section on page 7-7. | – |
| UDLD error detection | Enabled | “Configuring UniDirectional Link Detection” section on page 7-7 | – |
| UDLD error recovery | 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 5-25. | Reports |
| Switch Port Analyzer (SPAN) port monitoring | Disabled | “Configuring 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 4-4. 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 5-16 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> | – |
| Address 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 6-48. | Administration > SNMP |
| Community strings | public | <p>“SNMP Community Strings” section on page 5-16 and “Entering Community Strings” section on page 6-48.</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 |
| Port security aging | Disabled | “Configuring Port Security Aging” section on page 7-12. | – |
| Bridge Protocol Data Unit (BPDU) Guard | Disabled | “Configuring BPDU Guard” section on page 6-46. | – |
| Terminal Access Controller Access Control System Plus (TACACS+) | Disabled | “Configuring TACACS+” section on page 6-49. | – |
| Remote Authentication Dial-In User Service (RADIUS) | Disabled | “Controlling Switch Access with RADIUS” section on page 6-53. | – |

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.

