CHAPTER 4

# General Switch Administration

This chapter provides the following 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 about switch upgrades.

For information about the standard Cisco IOS Release 12.0 commands, refer to 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 it if you plan to use the 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)

Once IP information is assigned, you can run the switch on 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 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 release notes for the following 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 Configuration Changes" section on page 2-37. For information about saving changes from the CLI, see the "Saving Configuration Changes" section on page 3-10.

# Telnet Access to the CLI

The following procedure assumes you have assigned IP information and a Telnet password to the switch or command switch, as described in the release notes. 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.<br>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.<br>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. |
| **Step 6** | **end** | Return to privileged EXEC mode so that you can verify the entry. |
| **Step 7** | **show running-config** | Display the running configuration.<br>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. CMS requires that your switch uses HTTP port 80, which is the default HTTP port.

**Note** If you change the HTTP port, you cannot use CMS.

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.

Refer to the following 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 refer to the "Accessing CMS" section on page 2-35.

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 the following 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 5-22.

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 the following 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 the following 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***

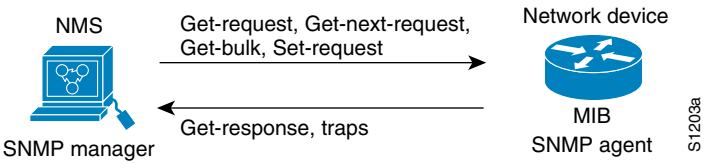


***Table 4-1 SNMP Operations***

| 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-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.

# 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 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 | None | "Designating and Enabling a Command Switch" section on page 5-14.<br>No CLI procedure provided. | VSM<br>**Cluster > Cluster Command Configuration** |
| Creating a cluster | None | "Creating a Switch Cluster" section on page 5-13.<br>No CLI procedure provided. | Cluster Builder |
| Adding and removing cluster members | None | "Adding and Removing Cluster Members" section on page 5-14.<br>No CLI procedure provided. | Cluster Builder<br>**Cluster > Add to Cluster** and **Cluster > Remove from Cluster** |
| Creating a standby command switch group | None | "Designating and Enabling Standby Command Switches" section on page 5-17.<br>No CLI procedure provided. | Cluster Manager:<br>**Cluster > Standby Command Configuration** |

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

| Feature | Default Setting | Concepts and CLI Procedures | CMS Option |
|---|---|---|---|
| Upgrading cluster software | Enabled | "Switch Software Releases" section on page 4-2.<br>Release notes on Cisco.com | Cluster Manager<br>**System > Software Upgrade** |
| Configuring SNMP community strings and trap managers | None | "SNMP Community Strings" section on page 5-10 and "Configuring SNMP" section on page 6-18. | Cluster Manager<br>**System > SNMP Management** |
| **Device Management** | | | |
| Switch IP address, subnet mask, and default gateway | 0.0.0.0 | "Changing IP Information" section on page 6-2.<br>Documentation set for Cisco IOS Release 12.0 on Cisco.com. | Cluster Manager<br>**System > IP Management** |
| Dynamic Host Configuration Protocol (DHCP) | DHCP client is enabled | "Using DHCP-Based Autoconfiguration" section on page 6-4.<br>Documentation set for Cisco IOS Release 12.0 on Cisco.com. | – |
| Management VLAN | VLAN 1 | "Management VLANs" section on page 8-4. | Cluster Manager<br>**Cluster > Management VLAN** |
| Domain name | None | "Configuring the Domain Name and the DNS" section on page 6-8.<br>Documentation set for Cisco IOS Release 12.0 on Cisco.com. | Cluster Manager<br>**System > IP Management** |
| Cisco Discovery Protocol (CDP) | Enabled | "Configuring CDP" section on page 6-22.<br>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 |
|---|---|---|---|
| Address Resolution Protocol (ARP) | Enabled | "Managing the ARP Table" section on page 6-45.<br>Documentation set for Cisco IOS Release 12.0 on Cisco.com. | Cluster Manager<br>**System > ARP Table** |
| System Time Management | None | "Setting the System Date and Time" section on page 6-17.<br>Documentation set for Cisco IOS Release 12.0 on Cisco.com. | Cluster Manager<br>**Cluster > System Time Management** |
| Static address assignment | None assigned | "Adding Static Addresses" section on page 6-59.<br>Documentation set for Cisco IOS Release 12.0 on Cisco.com. | Cluster Manager<br>**Security > Address Management** |
| Dynamic address management | Enabled | "Managing the MAC Address Tables" section on page 6-56.<br>Documentation set for Cisco IOS Release 12.0 on Cisco.com. | Cluster Manager<br>**Security > Address Management** |
| Voice configuration | – | "Configuring Voice Ports" section on page 7-17. | – |
| VLAN membership | Static-access ports in VLAN 1 | "Assigning VLAN Port Membership Modes" section on page 8-7. | Cluster Manager<br>**VLAN > VLAN Membership** |
| VMPS Configuration | – | "How the VMPS Works" section on page 8-52. | Cluster Manager<br>**Cluster > VMPS Configuration** |
| VTP Management | VTP server mode | "Configuring VTP" section on page 8-20. | Cluster Manager<br>**VLAN > VTP Management** |

*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 7, "Configuring the Switch Ports." | Cluster Manager<br>**Port > Port Configuration** and **Device > LRE Profile** (for LRE ports only) |
| Duplex mode | • Auto on all 10/100 ports<br>• Half duplex on all LRE ports | "Changing the Port Speed and Duplex Mode" section on page 7-2. | Cluster Manager<br>**Port > Port Configuration** |
| Speed on 10/100 ports | Auto | "Changing the Port Speed and Duplex Mode" section on page 7-2 | Cluster Manager<br>**Port > Port Configuration** |
| Gigabit Ethernet flow control | • Any on all Gigabit ports<br>• Disabled on LRE ports in half-duplex mode; enabled on LRE ports in full-duplex mode<br>**Note** This option is configurable only on the Gigabit ports. | "Configuring Flow Control on Gigabit Ethernet Ports" section on page 7-3. | Cluster Manager<br>**Port > Port Configuration** |
| LRE link speed and LRE port profiles | LRE-10 | "Configuring the LRE Ports" section on page 7-22. | Cluster Manager<br>**Device > LRE Profile Configuration** |
| Inline power | Auto | "Configuring Inline Power on the Catalyst 3524-PWR Ports" section on page 7-21 | – |

*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. | Cluster Manager **Port > Flooding Control** |
| Flooding unknown unicast and multicast packets | Enabled | "Blocking Flooded Traffic on a Port" section on page 7-6. | Cluster Manager **Port > Flooding Control** |
| Cisco Group Management Protocol (CGMP) | Enabled | "Controlling IP Multicast Packets through CGMP" section on page 6-46. | Cluster Manager **Device > Cisco Group Management Protocol (CGMP)** |
| Multicast VLAN Registration (MVR) | Disabled | "Configuring MVR" section on page 6-49. | – |
| Network Port | Disabled | "Enabling a Network Port" section on page 7-7. | – |
| **Network Redundancy** | | | |
| Hot Standby Router Protocol | Disabled | "Designating and Enabling Standby Command Switches" section on page 5-17. | – |
| Spanning Tree Protocol | Enabled | "Configuring STP" section on page 6-24. | Cluster Manager **Device > Spanning Tree Protocol (STP)** |
| Unidirectional link detection | Disabled | "Configuring UniDirectional Link Detection" section on page 7-9. | – |
| Port grouping | None assigned | "Creating EtherChannel Port Groups" section on page 7-10. | Cluster Manager **Port > Port Grouping (EC)** |

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

| Feature | Default Setting | Concepts and CLI Procedures | CMS Option |
|---|---|---|---|
| **Diagnostics** | | | |
| Displaying graphs and statistics | Enabled | "Displaying an Inventory of the Clustered Switches" section on page 5-19 and "Displaying Link Information" section on page 5-20. | Cluster Manager<br>**Port > Port Statistics** and **Port > Port Configuration > Runtime Status**<br>Cluster Builder<br>**Link > Link Graph** and **Link > Link Report** |
| Switch Port Analyzer (SPAN) port monitoring | Disabled | "Enabling SPAN" section on page 7-16. | Cluster Manager<br>**Port > Switch Port Analyzer (SPAN)** |
| Console, buffer, and file logging | Disabled | –<br>Documentation set for Cisco IOS Release 12.0 on Cisco.com. | – |
| Remote monitoring (RMON) | Disabled | "SNMP Network Management Platforms" section on page 4-6.<br>Documentation set for Cisco IOS Release 12.0 on Cisco.com. | – |
| **Security** | | | |
| Password | None | "Passwords" section on page 5-8 and "Changing the Password" section on page 6-15. | – |
| Addressing security | Disabled | "Managing the MAC Address Tables" section on page 6-56. | Cluster Manager<br>**Security > Address Management** |
| Trap manager | 0.0.0.0 | "Adding Trap Managers" section on page 6-19. | Cluster Manager<br>**System > SNMP Management** |

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

| Feature | Default Setting | Concepts and CLI Procedures | CMS Option |
|---|---|---|---|
| Community strings | public | "SNMP Community Strings" section on page 5-10 and "Entering Community Strings" section on page 6-19.<br>Documentation set for Cisco IOS Release 12.0 on Cisco.com. | Cluster Manager<br>**System > SNMP Configuration** |
| Port security | Disabled | "Enabling Port Security" section on page 7-14. | Cluster Manager<br>**Security > Port Security** |
| Terminal Access Controller Access Control System Plus (TACACS+) | Disabled | "Configuring TACACS+" section on page 6-61. | – |
| Protected port | Disabled | "Configuring Protected Ports" section on page 7-13. | – |