

# Switch Configuration Overview

---

This chapter provides an overview of the configuration and monitoring options supported by the Catalyst 1900 switch. Topics covered in this chapter are the following:

- Overview of the web console, including a list of the default configuration settings. Details are in the “Web-Based Management” chapter.
- Overview of the menu console, including a list of the default configuration settings. Details are in the “Menu-Based Management” chapter.
- Using an SNMP-compatible network management application and the switch Management Interface Base (MIB) files.
- Remote monitoring (RMON) concepts.

## Overview of the Web Console

The web console is a graphical user interface (GUI) for changing the switch configuration and monitoring network conditions and statistics. The web console is an embedded HTML web site in Flash memory. Online help is available on all pages.

---

**Note** HTTP is an in-band form of communication: you access the switch through one of its Ethernet or Fast Ethernet ports. Therefore, make sure that you do not disable or otherwise misconfigure the port through which *you* are communicating with the switch. You might want to write down the port number you are connected to. Make changes to the switch IP information with care.

---

# Accessing the Web Console

The switch must have an IP address before you can access the web console. See the “Assigning IP Information to the Switch” section on page 2-17.

To access the web console, follow these steps:

**Step 1** Start Netscape Communicator 4.xx or Internet Explorer 4.xx.

---

**Note** If you use Netscape 4.xx, enable JavaScript in the Advanced Preferences list. If you use Explorer 4.xx, JavaScript is enabled by default.

---

**Step 2** Enter the IP address of the switch in the URL field if you are using Netscape (the Address field if you are using Internet Explorer).

The home page of the web console, Basic System Configuration Page (shown in Figure 3-1), is displayed.

**Figure 3-1 Basic System Configuration Page**

Click Apply after making changes on a page. →

Click Revert to discard "unapplied" changes on a page. →

Click Help for help on a specific page. →

Click the Mode button to change the mode the LEDs display: port status, switch utilization, and port duplex operation. →

Click these topics to move from page to page. When the cursor is above a topic, a pop-up briefly describes the options on that particular page. (On Netscape only.)

Click a port to display its settings and statistics.

11195

You now can continue to configure or monitor the switch from the web console, as described in the “Web-Based Management” chapter.

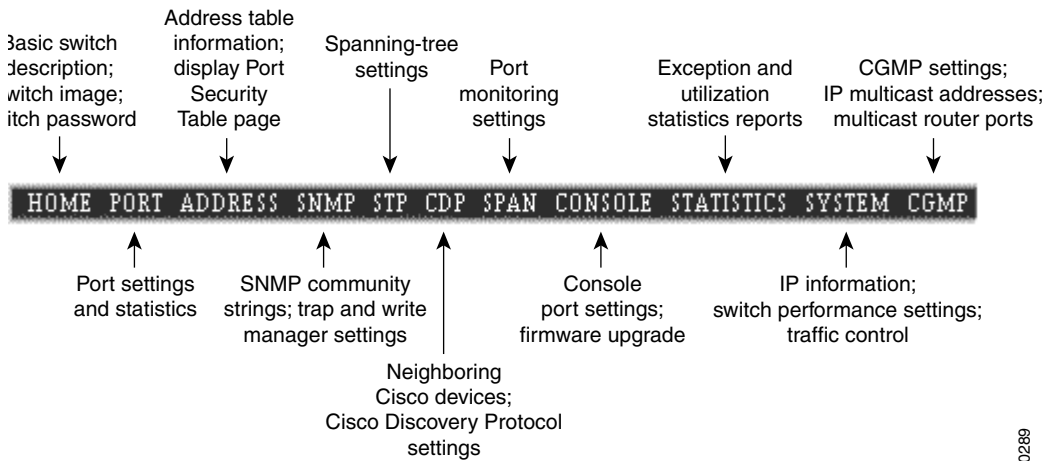
**Note** You can bookmark the IP address to easily retrieve the Basic System Configuration Page for later use. From the Netscape Communicator menu option, select Bookmarks, and then select Add Bookmark. From the Internet Explorer Favorites menu option, select Add to Favorites. Do not use the right mouse button to bookmark the web console; doing so only saves the specific frame (image) of the web console.

**Note** When you click the browser Reload button, or on some Sun and Macintosh platforms, when you resize the window, the browser redisplay a fresh copy of the Basic System Configuration Page.

## Navigating in the Web Console

You can use the action bar at the top of each page to move between pages. Figure 3-2 lists the functions for each action bar section.

**Figure 3-2 Web Console Action Bar**



10289

## Making Changes with the Web Console

Web console pages function much like other GUIs. A web console page displays the current settings for the switch. You then change the switch settings by entering information into fields, adding and removing list items, or selecting check boxes.

- Items added to or removed from web-console lists immediately become part of the running configuration. You do not need to click **Apply**.
- Changes (such as entering information in fields and selecting/deselecting check boxes) become part of the running (current) configuration after you click **Apply**.

After clicking **Apply**, you will not be able to revert to the previous settings.

- If you want to discard *all* your changes *and* if you have not clicked **Apply**, click **Revert**.

---

**Note** Wait approximately 30 seconds for the changes to be saved to permanent storage before turning off the switch, or the changes might not be saved.

---

You can restrict access to the menu console by using a password and locking out a user who fails to enter the password within a set number of attempts. The network administrator can then be alerted by in-band management messages. For information about setting the password, see the “Basic System Configuration Page” section on page 4-2.

## Using the Default Settings on the Web Console

The switch is designed to operate with little or no user intervention. In most cases, you can start using the switch with its default settings as soon as you assign an IP address to the switch.

Default values are defined for all switch features, and the switch begins forwarding packets as soon as it is powered up and connected to compatible devices. Table 3-1 shows the default values and the web console pages you use to change them.

## Overview of the Web Console

---

**Table 3-1**      **Features, Default Settings, and Console Pages**

<b>Feature</b>	<b>Default Setting</b>	<b>Web Console Page</b>
<b>Management</b>		
IP address, subnet mask, and default gateway to the switch	0.0.0.0	System Management Page
Cisco Discovery Protocol	Enabled	CDP Management Page
<b>Performance Tuning</b>		
Switching mode	FragmentFree (cut-through)	System Management Page
Enhanced Congestion Control (ECC) on 10BaseT ports	Disabled	System Management Page
Enhanced Congestion Control (ECC) on 100BaseT ports	Disabled	Port Management Page
Duplex mode on 10BaseT ports	Half duplex	Port Management Page
Half-duplex back pressure on 10BaseT ports	Disabled	System Management Page
Duplex mode on switched 100BaseFX ports	Half duplex	Port Management Page
Duplex mode on switched 100BaseTX port	Autonegotiate	Port Management Page
<b>Flooding/Traffic Control</b>		
Broadcast storm control	Disabled	System Management Page
Store-and-forward on multicast	Disabled	System Management Page
Network Port	None	System Management Page
CGMP	Enabled	CGMP Management Page
Flooding unknown unicast packets	Enabled	Port Management Page
Flooding unregistered multicast packets	Enabled	Port Management Page

**Table 3-1 Features, Default Settings, and Console Pages (Continued)**

<b>Feature</b>	<b>Default Setting</b>	<b>Web Console Page</b>
<b>Network Redundancy/Fault Tolerance</b>		
Spanning-Tree Protocol	Enabled	Spanning-Tree Management Page
Port Fast Mode Spanning-Tree Protocol on 10BaseT ports	Enabled	Spanning-Tree Management Page
Port Fast Mode Spanning-Tree Protocol on 100BaseT ports	Disabled	Spanning-Tree Management Page
<b>Diagnostics</b>		
Port monitoring	Disabled	SPAN Configuration Page
Remote monitoring	Enabled	—
Usage reports	—	Detailed Port Statistics Page Statistics Reports Page
<b>Security</b>		
Console password	None	Basic System Configuration Page
Action on address violation	Suspend	System Management Page
Addressing security	Disabled	Address Table Management Page Port Security Table Page
Define trap manager	None	SNMP Management Page
Define set (write) manager	None	SNMP Management Page
Community string	Public/Private	SNMP Management Page
<b>Upgrades</b>		
Firmware	—	Console and Upgrade Configuration Page

## Overview of the Menu Console

The menu console is a menu-driven interface for configuring and monitoring network conditions and statistics. You can use the menu console even when the network is down because the console bypasses the network and communicates directly with the switch.

## Accessing the Menu Console

To access the menu console, follow these steps:

**Step 1** Establish a connection with the switch by either:

- Connecting the console port to a management station or dial-up modem. For complete information, see the “Connecting to the Console Port” section on page 2-14.
- Using Telnet from a remote host. First, establish network connectivity between the switch and the Telnet client. You can use any Telnet TCP/IP package. The switch supports up to seven simultaneous Telnet sessions. Changes made by one Telnet user are reflected in all other Telnet sessions.

After you connect through the console port or through a Telnet session, the Menu Console Logon Screen is displayed (shown in Figure 3-3) on the console.

**Figure 3-3 Menu Console Logon Screen**

```
Catalyst 1900 Management Console
Copyright (c) Cisco Systems, Inc. 1993-1998
All rights reserved.
```

```
Standard Edition Software
Ethernet address:      00-E0-1E-7E-B4-40
```

```
PCA Number: 73-2239-01
PCA Serial Number: SAD01200001
Model Number: WS-C1924-A
System Serial Number: FAA01200001
-----
```

```
User Interface Menu
```

```
[M] Menus
[I] IP Configuration
```

```
Enter Selection:
```

**Step 2** Enter the [M] option to display the Management Console Main Menu (Figure 3-4).

**Figure 3-4 Management Console Main Menu**

```
Catalyst 1900 - Main Menu

[C] Console Settings
[S] System
[N] Network Management
[P] Port Configuration
[A] Port Addressing
[D] Port Statistics Detail
[M] Monitoring
[B] Bridge Group
[R] Multicast Registration
[F] Firmware
[I] RS-232 Interface
[U] Usage Summaries
[H] Help

[X] Exit Management Console

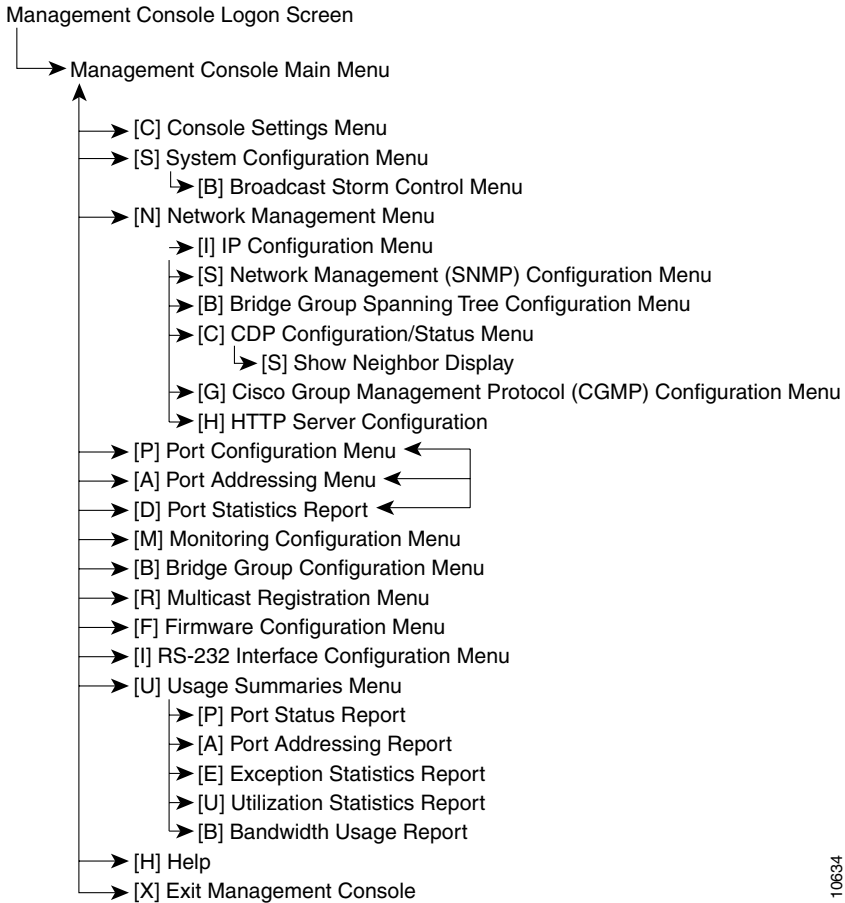
Enter Selection:
```

You now can continue to configure or monitor the switch from the menu console, as described in the “Menu-Based Management” chapter.

## Navigating in the Menu Console

Figure 3-5 lists the menus that are available from the Main Menu of the menu console.

**Figure 3-5 Menu Console Menus and Displays**



10634

## Making Changes with the Menu Console

When you use the menu console, keep the following in mind:

- When you change configuration settings, the changes take effect immediately. However, wait at least 30 seconds for the changed parameters to be written to permanent storage. Otherwise the changes do not take effect.
- You can restrict access to the menu console by using a password and locking out a user who fails to enter the password within a set number of attempts. The network administrator can then be alerted by in-band management messages. For information about setting the password, see the “Console Settings Menu” section on page 5-4.
- The information you enter is not case sensitive, except when entered as a descriptive string that preserves case.
- To select a menu, enter the letter in square brackets that precedes or follows the selection. You do not need to press Return.
- Enter an X to return to a parent menu. Enter an X on the Menu Console Logon Screen to exit the menu console and return to the command prompt.
- Menus display the current settings used by the switch, except when parameters are activated as a group. In certain cases, the settings are overridden by the settings on some menus and become active when those settings are turned off.
- Certain menus, such as the RS-232 Port Configuration Menu, allow activation of the given parameters as a group.
- The Backspace key works as expected; it erases the character previously entered.  
In addition, when the cursor is at the beginning of an entry, pressing the Backspace key clears the entry.
- Press Return after entering any parameters. When the cursor is at the beginning of an entry, pressing Return cancels the attempt, and the menu is redisplayed unchanged.

---

**Note** The menus and displays in this chapter are for reference only and might not exactly reflect the menus and displays on your console.

---

# Using the Default Settings on the Menu Console

The switch is designed to operate with little or no user intervention. In most cases, you can start using the switch with its default settings as soon as you assign an IP address to the switch.

Default values are defined for all switch features, and the switch begins forwarding packets as soon as it is powered up and connected to compatible devices. Table 3-2 shows the default values and the web console pages you use to change them.

**Table 3-2 Features, Default Settings, and Console Menus**

<b>Feature</b>	<b>Default Setting</b>	<b>Console Menu</b>
<b>Management</b>		
IP address, subnet mask, and default gateway to the switch	0.0.0.0	IP Configuration Menu
Cisco Discovery Protocol	Enabled	CDP Configuration/Status Menu
<b>Performance Tuning</b>		
Switching mode	FragmentFree (cut-through)	System Configuration Menu
Enhanced Congestion Control (ECC) on 10BaseT ports	Disabled	System Configuration Menu
Enhanced Congestion Control (ECC) on 100BaseT ports	Disabled	Port Configuration Menu (100BaseT Ports)
Duplex mode on 10BaseT	Half duplex	Port Configuration Menu (10BaseT Ports)
Half-duplex back pressure on 10BaseT ports	Disabled	Port Configuration Menu (10BaseT Ports)
Duplex mode on 100BaseFX port	Half duplex	Port Configuration Menu (100BaseT Ports)
Duplex mode on 100BaseTX ports	Autonegotiation	Port Configuration Menu (100BaseT Ports)
<b>Flooding/Traffic Control</b>		
Broadcast storm control	Disabled	System Configuration Menu
Network Port	None	System Configuration Menu
CGMP	Enabled	Cisco Group Management Protocol (CGMP) Configuration Menu
Overlapping bridge groups	Disabled	System Configuration Menu
Store-and-forward on multicast	Disabled	System Configuration Menu

**Table 3-2 Features, Default Settings, and Console Menus (Continued)**

<b>Feature</b>	<b>Default Setting</b>	<b>Console Menu</b>
Flooding unknown unicast packets	Enabled	Port Addressing Menu
Flooding unregistered multicast packets	Enabled	Port Addressing Menu
<b>Network Redundancy/Fault Tolerance</b>		
Spanning-Tree Protocol	Enabled	Spanning Tree Configuration Menu
Port Fast Spanning-Tree Protocol on 10BaseT ports	Enabled	Port Configuration Menu (10BaseT Ports)
Port Fast Spanning-Tree Protocol on 100BaseT ports	Disabled	Port Configuration Menu (100BaseT Ports)
<b>Diagnostics</b>		
Port monitoring	Disabled	Monitoring Configuration Menu
Remote monitoring (RMON)	Enabled	—
Usage reports	—	Port Status Report Port Addressing Report Exception Statistics Report Utilization Statistics Report Bandwidth Usage Report
<b>Security</b>		
Console password	None	Console Settings Menu
Action on address violation	Suspend	System Configuration Menu
Addressing security	Disabled	Port Addressing Menu
Define trap manager	None	Network Management (SNMP) Configuration Menu
Define set (write) manage	None	Network Management (SNMP) Configuration Menu
Community strings	Public/Private	Network Management (SNMP) Configuration Menu
<b>Upgrading</b>		
Firmware	—	Firmware Configuration Menu

# In-Band Management

You can configure and manage the switch by accessing the MIB objects through in-band management. This section provides the following information about in-band management through Simple Network Management Protocol (SNMP).

- Accessing the files with the MIBs and traps supported by the switch
- Accessing MIB variables using SNMP

---

**Note** Wait approximately 30 seconds for the changes to be saved to permanent storage before turning off the switch, or the changes might not be saved.

---

## Accessing MIB and Trap Information

These MIB files contain variables that can be set or read to provide information about the switch and the traps generated by the switch.

- RFC1213-MIB.my contains the MIB II (RFC 1213).
- BRIDGE-MIB.my contains the Bridge MIB (RFC 1493).
- ESSWITCH-MIB.my contains the Catalyst 1900 device-specific MIB.
- ETHERLIKE-MIB.my contains the MIB for Ethernet-like devices.
- CISCO-CDP-MIB-V1SML.my contains the Cisco Discovery Protocol (CDP) MIB.
- CISCO-MEMORY-POOL-MIB.my contains types of memory pools used by the switch.
- RS232-MIB-V1SML.my contains the RS-232 MIB (RFC 1317).

The switch is shipped with a DOS diskette containing the switch firmware and device-specific MIBs. You can also obtain a copy of the MIB files in the following ways:

- Using File Transfer Protocol (FTP) to access the ftp.cisco.com server.
- Using Cisco Connection Online (CCO) to access the cisco.com server.

### Using FTP to Access the MIB Files

To obtain a MIB file, follow these steps:

- 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 name when prompted for the password.
- Step 4** At the `ftp>` prompt, change directories to `/pub/MIBs`.
- Step 5** Use the `get README` command to display the readme file listing available files.
- Step 6** Use the `get MIB_filename` command to get a copy of the MIB file.

### Using CCO to Access the MIB Files

To access the MIB files from CCO, click **Software & Support** to display the Software Center site.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: <http://www.cisco.com>
- WWW: <http://www-europe.cisco.com>
- WWW: <http://www-china.cisco.com>
- Telnet: `cco.cisco.com`
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; data bits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact [cco-help@cisco.com](mailto:cco-help@cisco.com). For additional information, contact [cco-team@cisco.com](mailto:cco-team@cisco.com).

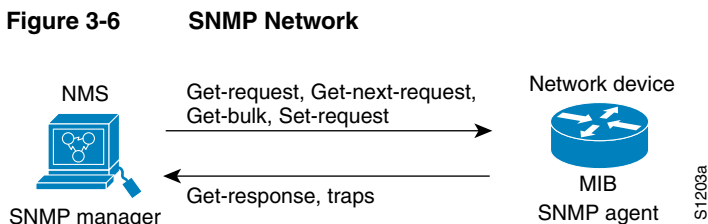
## Using SNMP to Access MIB Variables

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: SNMP manager, SNMP agent, and MIB.

SNMP places all operations in a *get-request*, *get-next-request*, and *set-request* format. For example, an SNMP manager can get a value from an SNMP agent or store a value into that SNMP agent. The SNMP manager can be part of a network management system (NMS), and the SNMP agent can reside on a networking device such as a switch. You can compile the switch MIB files with your network management software. The SNMP agent can respond to MIB-related queries being sent by the NMS.

An example of an NMS is the CiscoWorks network management software. CiscoWorks 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 in order to troubleshoot internetworking problems, increase network performance, verify the configuration of devices, monitor traffic loads, and more.

Figure 3-6 shows how the SNMP agent gathers data from the MIB, which holds information about device parameters and network data. The agent can send traps, or notification of certain events, to the manager.



---

**Note** Make sure you use the correct READ and WRITE community strings so that your SNMP request does not fail. Refer to the Network Management (SNMP) Configuration Menu for the correct community strings.

---

The SNMP manager uses information in the MIB to perform the operations described in Table 3-3.

**Table 3-3 SNMP Manager Operations**

Operation	Description
get-request	Retrieves a value from a specific variable.
get-next-request	Retrieves a value from a variable within a table. <sup>1</sup>
get-response	Reply to a get-request, get-next-request, and set-request sent by an NMS.
set-request	Store a value in a specific variable.
trap	Send an unsolicited message from an SNMP agent to an SNMP manager indicating that some event has occurred.

1. An SNMP manager does not need to know the exact variable name. It sequentially searches to find the needed variable from within a table.

## Remote Monitoring (RMON)

Remote Monitoring (RMON) is a standard monitoring specification that allows various network monitors and console systems to exchange network monitoring data. The switches provide support for the RMON of all ports. RMON provides you with visibility into network activity. You can access and remotely monitor the RMON specification RFC-1757 groupings of statistics, historical information, alarms, and events for any port through SNMP or through management applications, such as TrafficDirector.

RMON is enabled by default and is not displayed on the console. The switches support the statistics, history, alarm, and event groups.

The RMON feature monitors network traffic at the link layer of the OSI model without requiring a dedicated monitoring probe or network analyzer. You can analyze network traffic patterns, set up proactive alarms to detect problems before they affect users, identify heavy network users as candidates to move to dedicated or higher speed ports, and do trend analysis for long-term planning.

The switches support the following four RMON groups:

- Segment statistics
- Short- and long-term history
- Alarms
- Events

The statistics group of the RMON specification maintains utilization and error statistics for the monitored switch. Statistics include information about collisions, cyclic redundancy checks (CRCs) and alignment; undersized or oversized packets, jabber, fragments, broadcast, multicast, and unicast messages; and bandwidth utilization.

The history group takes periodic samples from the statistics section and stores them for later retrieval. This sampling includes information such as utilization, error counts, and packet counts.

You can use the alarm group to set a sampling interval and threshold for any RMON recorded item. Examples of alarm settings include absolute or relative values, rising or falling thresholds of utilization, packet counts, and CRC errors.

The events group allows events (generated traps) to be logged and provided to a network manager. The time and date are recorded with each logged event. You can use the events group to create customized reports that are based on alarm types.

With RMON enabled, the switches collect and forward comprehensive network traffic information from multiple Ethernet segments simultaneously. This capability allows you to obtain information to help tune or troubleshoot a switched LAN.

Extended RMON capabilities are provided through the use of a networking monitoring probe (such as Cisco SwitchProbe) connected to the monitoring (Switched Port Analyzer (SPAN)) port of the switch.