

Troubleshooting

There are several ways to troubleshoot installation and performance problems. For instance, the front-panel LEDs provide the quickest way to evaluate switch operation. The statistics provided by the switch management interfaces or SNMP management station can provide more details about connectivity and performance problems. The power-on self-test (POST) determines if the switch is functioning properly when powered up.

This chapter provides the following sections that describe potential problems and provide corrective actions:

- Diagnosing problems
- Understanding POST results
- Using the menu-based diagnostic console for switch recovery

Diagnosing Problems

Table 5-1 lists symptoms, possible causes, and corrective actions associated with

- Poor performance.
- No connectivity.
- No access to management interfaces.
- Cannot join a switch cluster.
- LED indications

Table 5-1 Common Problems and Their Solutions

| Symptom | Possible Cause | Resolution |
|--------------------------------------|---|---|
| Poor performance or excessive errors | <p>Incorrect full-duplex settings for 10BaseT and 100BaseT connections.</p> <p>Full-duplex status is shown with the Mode button and the FDUP LED.</p> <p>Check the port statistics:</p> <ul style="list-style-type: none"> • FCS and alignment errors on the port mean the switch port is configured for full-duplex operation and the other device is a repeater or half-duplex device. • Late collisions mean the port is configured for half-duplex operation and the attached device is full duplex. | <p>Configure the port for half-duplex operation.</p> <p>Configure the port for full-duplex operation.</p> |
| | <p>Cabling distance exceeded.</p> <p>Port statistics show excessive FCS, late-collision, or alignment errors. For 100BaseTX connections:</p> <ul style="list-style-type: none"> • The distance between the port and the attached device exceeds 100 meters. • If attached to a repeater, the total distance between the two end stations exceeds the 100BaseT cabling guidelines. <p>For 10BaseT connections: The distance between the port and the attached device exceeds 100 meters.</p> | <p>Reduce the cable length to within the recommended distances.</p> <p>See your 100BaseT repeater documentation for cabling guidelines.</p> <p>Reduce the cable length to within the recommended distances.</p> |
| | <p>Bad adapter in attached device.</p> <p>Excessive errors found in port statistics.</p> | <p>Run the adapter card diagnostic utility.</p> |
| No connectivity | <p>Incorrect or bad cable.</p> <ul style="list-style-type: none"> • A crossover cable was used when straight-through was required, or vice-versa. • Bad cable. | <p>See Appendix B, “Connectors and Cables,” for the correct pinouts and the proper use of crossover vs. straight-through cables.</p> <p>Replace with a known good cable.</p> |

Table 5-1 Common Problems and Their Solutions (continued)

| Symptom | Possible Cause | Resolution |
|---------------------------------|--|---|
| No management console access | Configuration problems. | Use the Diagnostic Console - System Debug Interface Menu to reset the switch. |
| | Incorrect baud rate. | Use the Diagnostic Console - System Debug Interface Menu to reset the modem parameters to their factory defaults. |
| Unable to join a switch cluster | CDP version 2 is not enabled on the switch. | Use the CDP Configuration/Status Menu to enable CDP version 2. |
| | Faulty connection to the command switch. | Use the [S] Show Neighbor option on the CDP Configuration/Status Menu, or use the CDP Management Page to display the devices connected to the switch. |
| | Command switch is not running IOS Release 12.0(5)XP software or higher. | Upgrade the command switch with the correct firmware. |
| | There are already 15 cluster members under the command switch. | Decide whether to replace an existing cluster member with the switch or to add the switch to a different switch cluster. |

Table 5-1 Common Problems and Their Solutions (continued)

| Symptom | Possible Cause | Resolution |
|---------------|---|---|
| | <p>Mismatched cluster configuration between the member switch and the command switch. Switch was removed from the cluster by using one of the following methods from the member switch:</p> <ul style="list-style-type: none"> • Using the [F] Reset to factory defaults option from the System Configuration Menu on the management console • Using the [R] Remove From Cluster option from the Cluster Management Menu on the management console • Using the [F] Return system to factory defaults option on the diagnostic console • Using the no cluster commander-address command from the switch CLI • Downgrading the switch firmware from the enterprise edition to the standard edition | <p>Note We recommend using the command-switch management interfaces to remove member switches from a cluster instead of using the previously mentioned methods (such as using the reset to factory defaults option from the management console).</p> <ul style="list-style-type: none"> • If you want to add the switch to a cluster but had used one of the previously mentioned methods to remove it from a cluster, you must use one of the command-switch management interfaces to remove and then add the switch. • Ensure the switch is not already a member switch of any cluster. Check this from the Cluster Management Menu on the management console and from the command switch (by using either the Cluster Builder application or the show cluster members command). For example, the MAC address of the command switch should be displayed from Cluster Management Menu on the switch management console, and the MAC address of the member switch should be displayed when you use the show cluster members command from the command switch CLI. |
| RPS LED amber | RPS not operational. | Verify that the RPS is connected properly to the switch and is connected to an AC power outlet. For information about the RPS, see the Cisco RPS documentation. |

Table 5-1 Common Problems and Their Solutions (continued)

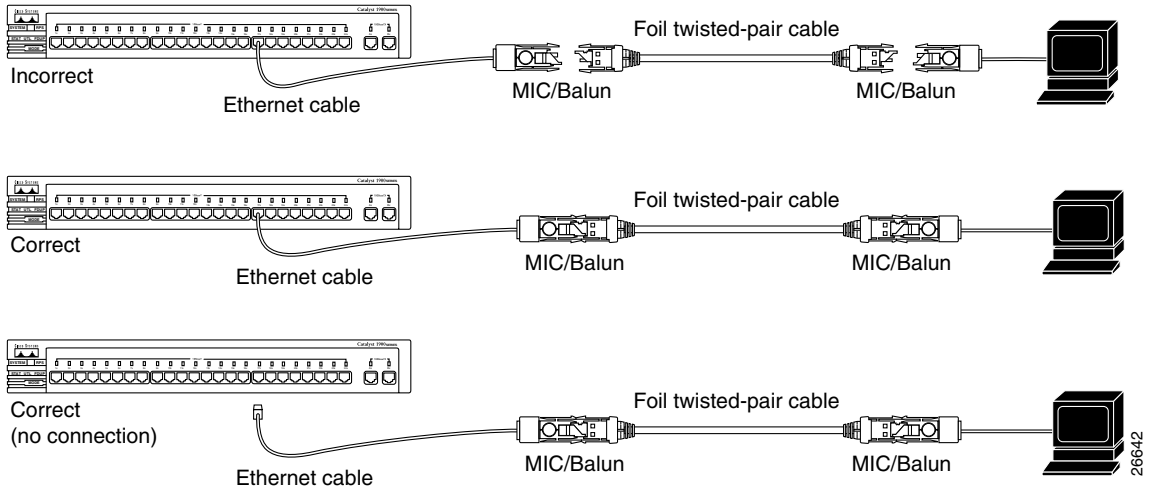
| Symptom | Possible Cause | Resolution |
|---|---|---|
| SYSTEM LED off | Power cord not connected. | Verify the connection of both ends of the power cord. |
| | Power supply failure. | <ul style="list-style-type: none"> • If you are using the switch internal AC power supply, contact your Cisco representative or reseller for support. • If you are using the Cisco RPS, replace the faulty RPS with a known good Cisco RPS. |
| SYSTEM LED is amber; port status LEDs off | Corrupt firmware. | See the “Recovering from Corrupted Firmware” section on page 5-13 of this chapter for firmware upgrade instructions. |
| Port LED off | Devices not powered up. | Ensure both devices have power. |
| | Cable connection loose. | Verify the connection at both ends of the cable. |
| | Wrong cable type. | Verify the cable type (crossover vs. straight-through). |
| | Incorrect wiring. | See Appendix B, “Connectors and Cables,” for pinout information. |
| | Faulty cable. | Replace the cable with a known good one. |
| Port LED alternating green and amber | Link fault. | <ul style="list-style-type: none"> • Check the connection between the switch port and the other device. • Check the operation of the connected device. |
| | Errors (such as excessive collisions, CRC errors, and alignment and jabber errors) could be affecting connectivity. | |
| Port LED amber | Port not forwarding. | <ul style="list-style-type: none"> • Check that the device that is connected to the disabled switch port is functioning properly. • Enable the port through in-band or out-of-band management. |
| | The port might be disabled by management, suspended because of an address violation, or suspended by Spanning-Tree Protocol because of the presence of network loops. | |

Avoiding Cabling Problems in Token-Ring Environments

Shielded twisted-pair cable is the most commonly used cable in Token-Ring environments. The media interface connectors (MICs) and baluns—used to connect shielded twisted-pair and unshielded twisted-pair cabling—create a loopback when they are disconnected; the loopback might cause anomalies with the switch.

To prevent loopback problems when using shielded twisted-pair cabling in a Token-Ring network environment, make sure the MICs and baluns are never left unconnected when they are part of a link connected to the switch (see Figure 5-1).

Figure 5-1 Shielded Twisted-Pair Cable Connections



266642

Understanding POST Failures

As described in the “Powering Up and Using POST to Test the Switch” section on page 2-6, the switch runs 13 tests each time it is powered up. This section provides information about fatal and nonfatal POST failures and recovery procedures.

If a nonfatal failure occurs, the SYSTEM LED is amber, and the switch is still operational and can forward packets, but it might not operate optimally. The Management Console Logon Screen displays the POST failure message that identifies the nonfatal failure(s) detected. For information about displaying POST results, see the “Starting Up the Switch and Displaying the POST Results” section on page 5-12.

If your switch has a fatal failure, the SYSTEM LED is amber, and one or more of the port LEDs are amber. The switch is not operational, but the amber port LED(s) indicate which test(s) failed.

Note Inform your system administrator about any POST failures. Contact your Cisco representative or reseller for support if any POST failures are detected.

Table 5-2 describes the individual tests and their associated LEDs.

Table 5-2 POST Test Descriptions

| Port LEDs | Test |
|------------------|--|
| 16x | Fatal—ECU DRAM test. Switch is not operational. |
| 15x | Not used during POST. |
| 14x | Not used during POST. |
| 13x | Not used during POST. |
| 12x | Fatal—Forwarding engine test. Switch is not operational. |
| 11x | Fatal—Forwarding engine SRAM test. Switch is not operational. |
| 10x | Fatal—Packet DRAM test. Switch is not operational. |
| 9x | Fatal—ISLT ASIC test. Switch is not operational. |
| 8x | Fatal—Port control/status test. Switch is not operational. |
| 7x | Fatal—System timer interrupt test. Switch is not operational. |
| 6x | Fatal—CAM SRAM test. Switch is not operational. |
| 5x | Nonfatal—Real-time clock test. If this test failed, the switch forwards packets. However, if the switch unexpectedly shuts down, it cannot restart itself automatically. |
| 4x | Nonfatal—Console port test. If this test failed, you cannot access the management console through the console port. You can still Telnet to the management console. |
| 3x | Fatal—Content addressable memory test. Switch is not operational. |
| 2x | Nonfatal—Built-in address test. If this test failed, the switch uses the default Ethernet address of the switch and begins forwarding packets. |
| 1x | Nonfatal—Port loopback test. If this test failed, some functionality to one or more ports is lost. The switch disables any port(s) that failed this test, and the failure message on the Management Console Logon Screen indicates which port(s) did not pass this test. Connect only to ports that passed this test. |

Recovery Procedures Using the Diagnostic Console

Note Access to the switch diagnostic console requires physical access to the switch.

The diagnostic console is a menu-drive interface that you can use to perform the following tasks:

- Start up the switch and display the POST results
- Recover from corrupted firmware
- Recover from a lost or forgotten password
- Reset the switch to factory defaults
- Reset the switch console port settings to the factory defaults

Accessing the Diagnostic Console

To display the diagnostic console, follow these steps:

- Step 1** Connect a management station with terminal emulation software (such as ProComm, HyperTerminal, tip, or minicom) supporting the XMODEM Protocol to the switch console port. For information about connecting to the console port, see the “Connecting to the Console Port” section on page 2-16.
- Step 2** Start up the emulation program.
- Step 3** Set the line speed on the emulation software to 9600 baud.

Note The recovery procedure runs at 9600 baud. To display the diagnostic console properly, make sure you set the line speed on the emulation software to 9600 baud.

- Step 4** Unplug the power cord from the back of the switch.
- Step 5** Press and hold in the Mode button, and at the same time, reconnect the power cord to the switch.
- Step 6** Release the Mode button 1 or 2 seconds after the LED above port 1x goes off. A display such as the one in Figure 5-2 appears.

Figure 5-2 Diagnostic Console Logon Screen

```
-----  
Cisco Systems Diagnostic Console  
Copyright(c) Cisco Systems, Inc. 1999  
All rights reserved.
```

```
Ethernet Address: 00-E0-1E-7E-B4-40  
-----
```

```
Press enter to continue.
```

Using the Diagnostic Console - Systems Engineering Menu

The Diagnostic Console - Systems Engineering Menu (Figure 5-3) provides options from which you can troubleshoot firmware problems and then restart the switch as usual.

To display this menu, press **Enter** from the Diagnostic Console Logon Screen.

Figure 5-3 Diagnostic Console - Systems Engineering Menu

```
Diagnostic Console - Systems Engineering

Operation firmware version: 9.00.00 Status: valid
Boot firmware version: 3.02

[C] Continue with standard system start up
[U] Upgrade operation firmware (XMODEM)
[S] System Debug Interface

Enter Selection:
```

Operation firmware version—The version of the switch firmware.

Status—Valid or invalid. If the firmware is not valid, the [C] Continue with standard system start up option is not displayed, and the following warning is displayed:

```
WARNING!!! Operation Firmware is invalid
Upgrade firmware to enable switch operation.
```

Boot firmware version—Current version of the write-protected part of the firmware that supports the diagnostic console.

[C] Continue with standard system start up—Use this option after you have resolved the firmware problems with the [U] Upgrade operation firmware (XMODEM) or [S] System Debug Interface option. The system exits the diagnostic console and restarts.

[U] Upgrade operation firmware—Initiate a firmware upgrade. This option works with XMODEM and uses the default RS-232 parameters: 9600 baud, 8 data bits, 1 stop bit, no parity, no flow control. You are prompted to choose a baud rate of 9600 or 57600 for the download. The console baud rate returns to 9600 immediately after the download.

Instead of using XMODEM, you can use 1KXMODEM to significantly reduce the download time.

[S] System Debug Interface—Display the Diagnostic Console - System Debug Interface Menu shown in Figure 5-5.

Starting Up the Switch and Displaying the POST Results

To display the POST results, enter the **[C] Continue with standard system start up** option from the Diagnostic Console - Systems Engineering Menu. For example, a POST failure message, such as the one in Figure 5-4, is displayed on the Management Console Logon Screen. In this example, ports 1x to 8x and port Ax (or port A) failed test 1 (nonfatal—port loopback test).

After you have resolved any firmware problems by using the **[U] Upgrade operation firmware (XMODEM) option** on the Diagnostic Console - Systems Engineering Menu to reinstall the firmware, use the **[C] Continue with standard system start up** option on the Diagnostic Console - Systems Engineering Menu to restart the switch.

If a nonfatal failure occurs, the SYSTEM LED turns amber.

Figure 5-4 Example of a POST Failure Message

```
Catalyst 1900 Management Console
Copyright (c) Cisco Systems, Inc. 1993-1999
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
-----
*** Power On Self Test (POST) failed ***
*** Failed Test(s): 1
*** Failed Port(s): 1 2 3 4 5 6 7 8 A
1 user(s) now active on Management Console.
Press any key to continue.
```

Recovering from Corrupted Firmware

Switch firmware can be corrupted during an upgrade, and it is possible to download the wrong file. In both cases, the switch does not pass POST, and there is no connectivity.



Caution If you interrupt the transfer by turning the switch off and on, the firmware could get corrupted.

Note When you download the firmware permanently to Flash memory, the switch does not respond to commands for approximately 1 minute. This is normal and correct. Do not turn off the switch until after the switch resets and begins using the new firmware.

From the diagnostic console, you can download the upgrade file from a management station to the switch by using the XMODEM protocol. The procedure for downloading the firmware through XMODEM is largely dependent on the terminal emulation software you are using.

To download the switch firmware by using the XMODEM protocol, follow these steps:

- Step 1** Copy the switch firmware from Cisco Connection Online (CCO) to a temporary area on your management station.
- New firmware releases can be downloaded from CCO, the Cisco Systems customer web site available at the following URLs: www.cisco.com, www-china.cisco.com, and www-europe.cisco.com.
- Step 2** Connect the management station that is using terminal emulation software (such as ProComm, HyperTerminal, tip, or minicom) that supports the XMODEM Protocol to the switch console port.
- Step 3** Start up the emulation program.
- Step 4** Set the line speed on the emulation software to 9600 baud.
- Step 5** Display the diagnostic console as described in the “Accessing the Diagnostic Console” section on page 5-10 and the “Using the Diagnostic Console - Systems Engineering Menu” section on page 5-11.
- Step 6** Enter the **[U] Upgrade operation firmware (XMODEM)** option from the Diagnostic Console - Systems Engineering Menu.

Recovery Procedures Using the Diagnostic Console

- Step 7** Enter **[Y]**es at the prompt to confirm the download:
- ```
Do you wish to continue with the download process, [Y]es or [N]o?
```
- It can take up to 1 minute to erase the existing firmware.
- Entering **[N]**o redisplay the Diagnostic Console - Systems Engineering Menu.
- Step 8** You are then prompted to choose a transmission speed. Enter **9** (for 9600) or **5** (for 57600):
- ```
Do you wish to upgrade at [9]600 (console speed) or [5]7600?
```
- After you select the transmission speed, the following prompt appears:
- ```
Waiting for image at the configured baud rate.
```

---

**Note** Change the baud rate of the management station to match the baud rate of the switch console port.

---

- Step 9** From your terminal emulation session:
- Select the XMODEM protocol option.
  - Enter the name of the switch upgrade file
  - Use the appropriate command to transfer the upgrade file to the switch.
- The system starts the XMODEM download.
- Step 10** When the upgrade is complete, the Diagnostic Console Logon Screen is displayed, and the switch returns to 9600 baud. Change the baud rate on the management station back to 9600 baud, if necessary.
- Step 11** Press **Return** to display the Diagnostic Console - Systems Engineering Menu, and enter the **[C]** **Continue with standard system start up** option from the Diagnostic Console - Systems Engineering Menu to restart the switch with the upgraded firmware.

### Recovering from a Lost or Forgotten Password

If you have lost or forgotten the switch password, you can clear the existing password and assign a new password.

To recover from a lost or forgotten password, follow these steps:

**Step 1** Power-cycle the switch.

After POST completes, the follow prompt is displayed:

```
Do you wish to clear the passwords? [Y]es or [N]o:
```

---

**Note** The switch waits 10 seconds for you to respond. If you do not, the switch automatically displays the Management Console Logon Screen. You cannot change the waiting period for answering this prompt.

---

**Step 2** Enter [Y]es to delete the existing password from nonvolatile RAM (NVRAM). You can then assign a password from the switch management interfaces (management console or CLI).

Entering [N]o maintains the existing password as valid.

---

**Note** If your switch is running boot firmware version 3.02 or earlier, the Diagnostic Console - System Debug Interface Menu includes the [V] View Management Console password option to display the switch password. This option is not available with boot firmware version 3.20 or higher. (See the “Using the Diagnostic Console - System Debug Interface Menu” section on page 5-16.)

---

### Using the Diagnostic Console - System Debug Interface Menu

The Diagnostic Console - System Debug Interface Menu (Figure 5-5) provides system options for resetting the console port or the entire switch to the factory defaults.

To display this menu, enter the **[S] System Debug Interface** option from the Diagnostic Console - Systems Engineering Menu.

**Figure 5-5 Diagnostic Console - System Debug Interface Menu**

```
Diagnostic Console - System Debug Interface

[G] Generic I/O
[M] Memory (CPU) I/O
[F] Return system to factory defaults
[R] Reset main console RS232 interface to 9600,8,1,N
[P] POST diagnostic console

[X] Exit to Previous Menu

Enter Selection:
```

---

**Note** If your switch is running boot firmware version 3.02 or earlier, the Diagnostic Console - System Debug Interface Menu includes the [V] View Management Console password option to display the switch password. This option is not available with boot firmware version 3.20 or higher.

---

**[G] Generic I/O**—For Cisco personnel only.

**[M] Memory (CPU) I/O**—For Cisco personnel only.

**[F] Return system to factory defaults**—Return the switch to its factory settings. All static and dynamic addresses are removed, as are the IP address and all other configurations. Enter **[Y]**es or **[N]**o, and press **Return**. The changes take effect when the switch is reset.

---

**Note** If the switch is a cluster member, using the **[F] Return system to factory defaults** option removes the switch from the cluster.

We recommend using the command-switch management interfaces to remove member switches from a cluster. If you want to add the switch to a cluster but had previously used the **[F] Return system to factory defaults** option to remove it from a cluster, you must use one of the command-switch management interfaces to remove and then add the switch.

---

**[R] Reset main console RS232 interface to 9600, 8, 1, N**—Use this option if you have lost the management console connection because of an improper modem configuration. When the switch is reset, the default RS-232 configuration is used.

**[P] POST diagnostic console**—For Cisco personnel only.

### Resetting the Switch to the Factory Defaults

There can be times when you need the diagnostic console even though the firmware is valid. This could happen, for example, if the switch configuration prevents the firmware from executing properly and you cannot display the management interfaces.

---

**Note** If the switch is a cluster member, using the [F] Return system to factory defaults option removes the switch from the cluster.

We recommend using the command-switch management interfaces to remove member switches from a cluster. If you want to add the switch to a cluster but had previously used the [F] Return system to factory defaults option to remove it from a cluster, you must use one of the command-switch management interfaces to remove and then add the switch.

---

To reset to the switch to the factory defaults, follow these steps:

**Step 1** Enter the [F] **Return system to factory defaults** option from the Diagnostic Console - System Debug Interface Menu.

The following prompt is displayed:

```
Return system to factory defaults? [Y]es or [N]o:
```

Entering [N]o redisplay the Diagnostic Console - System Debug Interface Menu.

**Step 2** Enter [Y]es.

## Resetting the Switch Console Port to Factory Defaults

To reset to the switch console port to the factory defaults, follow these steps:

**Step 1** Enter the **[R] Reset main console RS232 interface to 9600,8,1,N** option from the Diagnostic Console - System Debug Interface Menu.

The following prompt is displayed:

```
Return system to factory defaults? [Y]es or [N]o:
```

Entering **[N]o** redisplay the Diagnostic Console - System Debug Interface Menu.

**Step 2** Enter **[Y]es**.

