



System Troubleshooting Guidelines

This chapter explains how to isolate problems in the Cisco Integrated Communications System (ICS) 7750 (Cisco ICS 7750). It contains the following sections:

- [Finding the Source of a Problem, page 2-1](#)
- [Using Log Files for Troubleshooting, page 2-8](#)
- [Best Practices for Using the Cisco IOS CLI, page 2-14](#)
- [Obtaining Additional Troubleshooting Information, page 2-15](#)
- [Contacting the Cisco TAC, page 2-25](#)



Note

For a description of the features, modifications, and caveats for the Cisco Integrated Communications System 7750 (Cisco ICS 7750) release 2.6.0, refer to the [Release Notes for System Software Release 2.6.0 on the Cisco ICS 7750](#).

Finding the Source of a Problem

Use the information in this section to help isolate faults. You can perform these procedures before, after, instead of, or in addition to running the diagnostic software. However, these instructions are the only means of identifying faults in subsystems that are not covered by a power-on self-test (POST) or diagnostics, such as fans and power supply modules.

Some procedures must be performed on site, and others can be performed remotely.

This section is organized as follows:

- [Connection Problems](#)
- [Electrical Problems](#)
- [Temperature Problems](#)
- [Configuration Problems](#)
- [Signal Input/Output Problems](#)

Connection Problems

Before running diagnostics or attempting complex troubleshooting, verify the following:

- System power cord(s) and data cables are firmly connected at both ends.
- All system cards are firmly seated in the backplane and screwed securely to the chassis.
- The power supply modules and the fan tray are properly connected and screwed securely to the chassis.

Electrical Problems

Electrical problems are divided into two categories:

- [Site Electrical Problems](#)
- [Cisco ICS 7750 Electrical Problems](#)

Site Electrical Problems

Site electrical problems can include

- Improperly grounded equipment, particularly equipment racks and power grounds
- Fluctuating voltage, which can result from excessive power drains caused by other equipment (such as air-conditioning units)

- Cable corrosion or defective power panels, circuit breakers or fuses, or cable connections
- Undersized power cables or excessive power cable lengths
- Excessive power demand on backup power systems or batteries when alternate power sources are used

Cisco ICS 7750 Electrical Problems

System electrical problems can be caused by

- Improperly grounded equipment, particularly equipment racks and power grounds
- Improper power cable connections to the system
- Improper installation of power supply modules
- Circuit breakers that have tripped or that are defective
- Defective UPS (if installed)



Note

For installation instructions, refer to the [Cisco ICS 7750 Installation and Configuration Guide](#).

Temperature Problems

The Cisco ICS 7750 powers down when the temperature exceeds a specified threshold. If that happens, you should identify and correct the cause of the overheating before you reapply power to the system. Possible causes include the following:

- Environmental problems where the Cisco ICS 7750 is installed, such as insufficient air conditioning to keep the air ambient temperature between 32 and 104° F (0 to 40° C)
- Blockage of the system air intake or exhaust
- System fan or power supply failure

Configuration Problems

ICSConfig is an excellent overall troubleshooting tool. Through a GUI-based interface, ICSConfig reports networking and system card discovery problems, using specific error codes. When an error occurs, ICSConfig displays a page that contains a description of the specific error with links to the help pages that provide instructions for correcting the problem. If an error occurs while running ICSConfig, click the link(s) on the error code page for instructions on resolving the error condition, and then proceed with ICSConfig.

When powering up a card or interface (port) for the first time, a potential source of problems is improper configuration. The problem may exist at either the local side or the remote side of the connection; be sure to check both configurations.



Note

Refer to the [Cisco ICS 7750 Installation and Configuration Guide](#) for information on configuring nodes, cards, and interfaces.

Duplicate IP Address Problems

Ensure that no two network devices (such as Cisco ICS 7750 system cards, other network hosts, and Cisco IP Phones) are assigned the same IP address. If two network devices have the same IP address, you will encounter a duplicate IP address conflict, which will render one of your devices unusable.

If two network devices have the same IP address, the ICSConfig user interface will discover and report a duplicate IP address problem (see the [“Specific Duplicate IP Address Problem on the System Switch Processor \(SSP\)”](#) section on page 2-5). For informational purposes, you can also view the multi.log file, which will indicate the existence of a duplicate IP address. Output similar to the following will appear in the multi.log file after you invoke ICSConfig and ICSConfig has reported the appropriate error code:

```
06/12 01:24:59.206PM {ID.exe|Main}: GetSlotPresent: '6' is 'present'
06/12 01:24:59.206PM {ID.exe|Main}: GetLastCode[6]:
Discovery_Duplicate_IP 10.0.0.2
```

If you discover that two devices are using the same IP address, change the IP address of one of the devices to a different, unique IP address immediately in order to resolve the duplicate IP address conflict.



Note See the “[System Card Discovery and Bootup Problems](#)” section on page 2-10 for additional information about the multi.log file.

Specific Duplicate IP Address Problem on the System Switch Processor (SSP)

Under certain conditions, ICS System Manager may report a duplicate IP address for the SSP in the ICSSConfig user interface. This will be reported as error code 102:

```
Error Code: 102
Cannot discover SSP. SSP (IP Address) is not reachable from SPE
running System Manager (IP Address, Subnet Mask).
```

The problem might occur if another device in your network is configured with an IP address that is the same as the IP address configured for the SSP.

If the duplicate IP address is resolved by changing the IP address of the affected device, the ICSSConfig user interface may fail to recognize that the problem has been corrected. In this case, ICSSConfig will continue to report a duplicate IP address for the SSP.

If you encounter this problem, restart the Inventory Discovery process that runs on the SPE running System Manager.

To resolve this problem, restart Inventory Discovery by stopping and restarting FMMServer. Follow these steps:

-
- Step 1** Access the SPE310 Windows user interface, and connect your peripherals as described in the “[Accessing the SPE310 Windows Interface Through Terminal Services Client](#)” section on page 4-3.
 - Step 2** Log in as an administrator (userID *administrator*), and enter your password (the default is *changeme*).
 - Step 3** Stop the FMMServer on the SPE running System Manager:

```
net stop FmmServer
```
 - Step 4** Start FmmServer:

```
net start FmmServer
```

Step 5 Run ICSConfig. It should discover all cards in the chassis.

Signal Input/Output Problems

Signal input and output problems can occur at any point in the network and can be caused by mechanical defects in the cables, poor connections, or lack of signal caused by other equipment failures.

This section describes how to isolate problems with the following:

- [Node Connections](#)
- [Console Port Serial Connections](#)
- [Ethernet Connections](#)

Refer to your site log and other facility records to check signal connections for your facility.

Node Connections

You can use the **ping** command to determine whether you can communicate over a particular IP connection. The **ping** command sends Internet Control Message Protocol (ICMP) echo packets to the specified IP address and receives a confirmation if the connection is good.

Console Port Serial Connections

If the console screen that is connected to the system alarm processor (SAP) console port appears frozen or fails to work properly, check for the following problems:

- Make sure that the console cable is properly connected to the correct console port on the SAP at one end and to your terminal at the other end.
- Verify that you are using the correct type of cable and adapter. For information about pinout connections, as well as general installation instructions, refer to the [Cisco ICS 7750 Installation and Configuration Guide](#).

- Make sure that the cable is not defective or broken. Replace the cable with another high-quality cable, if necessary. Then observe whether the console port starts working.

**Note**

For detailed instructions on how to solve problems related to serial connections, see [Chapter 6, “Solving Serial Connection Problems.”](#)

Ethernet Connections

If the STATUS LED on the system switch processor (SSP) is not on, look for the following:

- Cable connections—Verify that an Ethernet cable is connected to the correct SSP interface and that there is a good connection on both ends of the cable.
- Defective or broken cable—Replace the cable with a known reliable Ethernet cable, and verify that the STATUS LED comes on.
- Cable type—Ensure that the proper type of cable is installed.
- SSP not booted—The SSP STATUS LED should be on. If necessary, remove and reinsert the SSP, and boot it up again. Refer to [Cisco ICS 7750 FRU Installation and Replacement](#) for removal and reinsertion instructions.

**Caution**

You can install only one SSP card in a single chassis. If you must hot swap the SSP, the system loses LAN connectivity. Calls being made from or to Cisco IP Phones routed through that SSP are disconnected until an operational SSP is properly reinserted in the chassis.

If the SSP STATUS LED is on, but one of its Ethernet interfaces does not seem to be working properly, make sure that the interface in question is configured properly and is not administratively shut down. If you have a working console connection, do the following:

-
- Step 1** At the Cisco IOS command prompt, enter **show interface ethernet** [*slot | interface*], specifying a slot containing an analog station interface (ASI), a multiservice route processor (MRP), or the SSP.

If the interface is down administratively, enter this command to enable it:

```
7750#configure terminal
```

Then enter configuration commands, one per line, and end with **Ctrl-z**.

For example:

```
7750(config-if)#int eth slot |interface
7750(config-if)#no shut
7750(config-if)#exit
7750(config)#Ctrl-z
7750#
```

Step 2 Verify that the Ethernet interface has a valid IP address assigned to it.

For more information about configuring Ethernet interfaces, refer to the [Cisco ICS 7750 Installation and Configuration Guide](#).

If the cable, connections, power, and configuration are normal, and you still cannot connect to the Ethernet interface on the SSP, replace the SSP. If the problem persists, contact Cisco's Technical Assistance Center (TAC) for further assistance.

**Note**

For instructions on how to solve problems related to Ethernet connections, including a detailed explanation of the **show interfaces ethernet** command output, see [Chapter 7, "Solving Ethernet Problems."](#)

Using Log Files for Troubleshooting

This section describes log file information as well as the Cisco IOS commands that you can use to obtain additional data for troubleshooting.

Troubleshooting Data from the SPE

A utility batch file, *copylogfiles.bat*, is provided as part of the ICS System Software installation package. This batch file is available under the C:\Program Files\Cisco Systems\ICS\Program directory. When executed on the SPE running System Manager, copylogfiles.bat saves all of the required logs and consolidates the necessary log information into one directory in the event of system errors.

If you encounter an error or problem on the Cisco ICS 7750, navigate to **C:\Program Files\Cisco Systems\ICS\Program** and double-click **copylogfiles.bat**; this action runs the utility and copies all of the relevant log files to one directory (C:\ICSSMLogs). This directory can then be zipped and sent to your Cisco support representative for problem determination and resolution.

Individually, the following files from the SPE can be used for troubleshooting:

- C:\Program Files\Network Registrar\BIN\ics_nrcmd.cfg
- C:\Program Files\Network Registrar\LOGS\name_dhcp_1_log
- C:\Program Files\Cisco System\ics\program*.log
- C:\Program Files\Cisco Systems\ics\Program\BBtrace.log
- C:\Program Files\Cisco Systems\ics\fm\Trace*.*
- C:\Program Files\network registrar\logs*.*
- C:\Program Files\network registrar\logs\ics_lease.out
- C:\W2KS\snmpdb.log
- Files in the directory C:\Program Files\Cisco\tftppath

The following are additional sources of information:

- Use the command prompt, and run **ipconfig /all**.
- Check the Windows application logs.
- Check the Windows system logs.



Note

For additional information on Cisco ICS 7750 log files, see the [“ICS System Manager Log Files”](#) section on page 5-4.

Troubleshooting Information from the SSP

You can use the following Cisco IOS commands on the SSP for troubleshooting information:

- **show mac-address-table**
- **show cdp neighbors detail**
- **show arp**
- **show ip arp**

CNR Troubleshooting Information

For Cisco Network Registrar (CNR) troubleshooting (for example, if a card is failing to get an IP address), check the following:

- Make sure that the ICSAddrSvc is started.
- C:\Program Files\network registrar\logs\name_dhcp_1_log. See the dhcp/bootp server start up and bind to port, and check that requests come in and are answered.
- C:\Program Files\network registrar\logs\ics_lease.out. Check leases for all devices (phones, PCs, and so on). An easier way to see this is to look at C:\Program Files\network registrar\bin\lease_list.out
- C:\Program Files\network registrar\bin\ics_nrcmd.cfg. The CNR configuration is generated from the database each time the Fault Management Module (FMM) starts.

System Card Discovery and Bootup Problems

In addition to the excellent troubleshooting resource that is provided by ICSCfg (see the “[Configuration Problems](#)” section on page 2-4) during discovery of the Cisco ICS 7750 system cards, you can also check the following logs for additional troubleshooting information:

- C:\Program Files\Cisco Systems\ics\Program\multi.log. This log shows you the ongoing discovery process for each card in the chassis.

- C:\Program Files\Cisco System\ics\Program\back.log. This log shows you older information that has been moved from the multi.log after that log fills up.

MRP Discovery and Bootup Problems

Check the following for MRP discovery and bootup problems:

- Capture bootup sequence via a hypterminal connection to console into the SAP. This should tell you whether the MRP is receiving a valid IP address, TFTP server, Cisco IOS image name and configuration (.cfg file).
 - If the MRP is not receiving any of these items, look at the CNR logs using a Terminal Services connection or a direct connection into the SPE. CNR logs can be found at C:\Program Files\Network Registrar\Logs.
 - If the MRP is receiving a response, look to see whether the MRP image exists in C:\Program Files\Cisco\TFTPPath. Be aware that the MRP image could be in a different location from the default path if Cisco CallManager is installed on the SPE. In that case, you can try to search the SPE for the .cfg file by choosing, on the SPE, **Start > Search > For Files or Folders**. In the dialog box **Search for files or folders named**, enter ***.cfg** and click **Search Now**.
- To further troubleshoot errors in the MRP configuration information, check C:\Program Files\Cisco Systems\ics\Program\BBtrace.log.
- Check the MRP card discovery/boot problems information in the following logs:
 - C:\Program Files\Cisco Systems\ics\Program\multi.log. This log shows the ongoing discovery process for each card in the chassis.
 - C:\Program Files\Cisco System\ics\Program\back.log. This log shows older information that has been moved from the multi.log when that log fills up.

See the [“Troubleshooting Cisco ICS 7750 Booting Problems”](#) section on page 3-32 for additional information.

Services Troubleshooting Information

When services such as Cisco CallManager fail to start, do the following.

- Check the C:\W2KS\system32\drivers\etc\hosts file. It should contain at least two entries, 127.0.0.1 (local host) and the IP address of the system processing engine (SPE) with its exact name.
- Check Windows application logs.
- Check Windows system logs.

FMM Troubleshooting

FMM is a software module that runs as a service on SPE cards in the Cisco ICS 7750. FMM is responsible for providing the fault detection and recovery mechanisms in the system, while also enabling the ICS System Manager application to monitor the status of SPEs, the SAP, and the chassis.

Check the following files when you need to troubleshoot issues with FMM:

- C:\Program Files\Cisco Systems\ics\fm\Trace*.*. This file does not capture information that spans a long period of time because the log information is overwritten. The file traces at level 7, the lowest level of debugging. You can change this with the HKLM\Software\FaultManagementModule\LogFile\Threshold key.
- You can view all FMM commands that have been invoked within the Cisco ICS 7750 and display those commands on another PC, using the FMMSyslog client (FMMSysLog.exe). To set up FMMSysLog.exe, see the [“Using the Fault Management Module”](#) section on page 2-17.

FMMSysLog.exe can be set up to display on another SPE (if available) or on a PC or system that is running Windows 2000 or Windows NT.

- To check the IP address configuration of the SPE, from a hyperterminal connection via the console port, issue these commands:

```
netsh
int ip
dump
```

- To check for duplicate IP addresses in the system, look for messages in the Event Viewer (**Start > Programs > Administrative Tools > Event Viewer**).
- To check MAC addresses if multi.log does not show the MatchMacAddress, on the SSP, run the Cisco IOS command **show mac-address-table**.

Database Tables

Microsoft SQL Server 2000 is used to store database information on the Cisco ICS 7750 SPE. There are several database tables that store information. The types of information stored in these database tables include the following.

- Historical record of software images used by each card in the Cisco ICS 7750 chassis
- Software image currently installed on each card
- Historical information of every component that has been installed in the system, with IP address and slot information
- Entries for syslog.conf, each MRP's configuration location, the location of the CNR IP address allocation file, and the DHCP lease information
- Software delivered to each card in the chassis
- Software agreement information for Event Manager setup
- Syslog messages
- List of host names for the SPEs in the chassis
- Enterprise-wide data and IP addresses of the SPEs



Caution

The database tables should be used with extreme caution. They may be viewed only. Do not make any manual changes to the information in the database tables because you may compromise the integrity of the system, corrupt the database, and render the system unusable. All system modifications should be made using ICS System Manager or Cisco CallManager administration tools.

Best Practices for Using the Cisco IOS CLI

ICS System Manager is designed to communicate with, and monitor the status of, all the components in the chassis. To enable ICS System Manager to perform these functions, a configuration program (ICSCConfig) provides the capability to easily configure key system parameters, such as the IP addresses of system cards, passwords, destination for syslog messages, and Simple Network Management Protocol (SNMP) community strings.

To enable ICS System Manager to perform all of its functions as a system management tool, it is important that you use ICSCConfig or ICS System Manager, as appropriate, rather than the Cisco IOS command-line interface (CLI), when you enter key system parameters.

With the exception of the procedures listed below, you can enter all the Cisco IOS CLI commands that are available for use in any Cisco IOS software release that is intended for use on the Cisco ICS 7750.

You should always use ICSCConfig for the following tasks:

- Passwords
 - Changing the login password, which gives ICS System Manager continued Telnet access to system cards
 - Changing the Windows 2000 administrator password, which grants those with administrator privileges continued access to SPE310s
 - Changing the enable or secret password, which makes it possible for administrators to enter certain Cisco IOS commands
- Card configurations
 - Assigning or changing the IP addresses or subnet mask of system cards
- SNMP settings
 - Changing read-only and read/write SNMP community strings of the SNMP server
 - Changing the server destination of SNMP traps
 - Managing the SNMP server
- Logging
 - Changing the syslog logging host

**Note**

SNMP community strings and system passwords are case-sensitive, and should be configured only through ICSCConfig.

The following tasks cannot be performed on the Cisco ICS 7750 using the Cisco IOS CLI under any circumstances:

- Shutting down an Ethernet interface
- Changing the IP address of a Fast Ethernet interface (unless you have configured VLAN support)
- Disabling Cisco Discovery Protocol (CDP) on an Ethernet or VLAN interface

The following tasks cannot be performed on the SPEs under any circumstances:

- Configuring Domain Name System (DNS) on SPEs
- Invoking the Cisco Network Registrar (CNR) dhcp.exe from `c:\program files\network registrar\bin`

Obtaining Additional Troubleshooting Information

This section describes additional sources of information that can help you solve system problems:

- [Using Diagnostic Commands](#)
- [Using Cisco Network and Fault Management Tools](#)
- [Using the Fault Management Module](#)
- [Using Third-Party Troubleshooting Tools](#)

For additional information on troubleshooting relating to known system caveats and workaround solutions, refer to the [Release Notes for System Software Release 2.6.0 on the Cisco ICS 7750](#).

Using Diagnostic Commands

System diagnostic commands can provide additional information that can help you solve problems. For more information about diagnostics, see the [“Performing Diagnostics” section on page 3-2](#).

Using Cisco Network and Fault Management Tools

CiscoWorks2000 includes a suite of fault management applications for diagnosing problems on the SNMP devices on your network. These applications include

- **Path Tool**—Graphically displays the route of a path from a source device to a destination device.
- **Real-Time Graphs**—Monitors the behaviors of device interfaces or other network elements suspected of operating in a degraded mode, and displays them in a graph.
- **Show Commands**—Display data similar to output from EXEC **show** commands.
- **Health Monitor**—Provides information about the status of a device and access to several CiscoWorks2000 applications in one window (including Show Commands and Real-Time Graphs) for monitoring SNMP device activity.
- **Contacts**—Provides quick access to the emergency contact person for a particular device.
- **Log Manager**—Enables you to store, query, and delete messages gathered from CiscoWorks2000 applications and Cisco Systems devices on the network.

[Table 2-1](#) identifies CiscoWorks2000 applications that can help you troubleshoot network problems.

Table 2-1 Troubleshooting with CiscoWorks2000

Problem	CiscoWorks2000 Application Recommendation
Network device	<ul style="list-style-type: none"> • Use Path Tool to check the graphical path for link utilization analysis. • Use Show Commands to get important data, such as the version and interface, for later analysis. • Check the Log Manager file for event information.
Protocol	<ul style="list-style-type: none"> • Check the Log Manager file for event information. • Use Path Tool to determine whether the protocol is routing efficiently. • Use Real-Time Graphs to get information on router traffic. • Use the show traffic mix command to view packet information.
Device configuration	<ul style="list-style-type: none"> • Use the show version command to ensure that version numbers are compatible. • Log in to the device, and determine whether the device configuration file has a read/write community string. • Use the show interface and show traffic mix commands to verify that the device is running. • Determine whether a configuration file with syntax errors was downloaded to a device. Log in to the console, and initiate a TFTP session from the device. The errors will be displayed on your console screen. Or, log in to the device before you download a file, and look for error messages.

Using the Fault Management Module

Components in the FMM module report events/errors through syslog messages and specific event log messages are written to the FMM log directory. You can view the entries in the FMM log, or you can view FMM syslog messages in real time by using the FMMSysLog client application.

To use the FMMSysLog Client to view syslog messages in real time, perform the following steps:

-
- Step 1** On a PC networked with the Cisco ICS 7750, Telnet to port 5000.

Obtaining Additional Troubleshooting Information

```
Telnet <IP address> 5000
```

where *IP address* is the address of the SPE running System Manager.

- Step 2** Log in as an administrator (user ID *administrator*), and enter the administrator password (default password is *changeme*).
- Step 3** On the SPE running System Manager, navigate to **C:\Program Files\Cisco Systems\ics\fmm**.
- Step 4** Open the file **C:\Program Files\Cisco Systems\ics\fmm\FmmSysLog.exe** on the target SPE, and copy this file to another PC.
- Step 5** Register the client by running the following command:

```
C:\Program Files\Cisco Systems\ics\fmm>fmmcli registersyslogclient
-ipaddress <PC's IPaddr> -level 7
```

where *IP address* is the address of the PC or system on which you wish to see all the FMM commands, and where the *level* is a range from 0 through 7, signifying the following:

- 7 = All commands (debugging level, captures all information)
- 6 = Informational
- 5 = Notifications
- 4 = Warnings
- 3 = Errors
- 2 = Critical
- 1 = Alert
- 0 = Emergencies

The following is an example of the command and the output that is displayed on the monitor attached to the SPE after the RegisterSyslogClient command is processed successfully:

```
C:\Program Files\Cisco Systems\ics\FMM>fmmcli RegisterSyslogClient
-ipaddress 192.168.1.200 -level 7
```

```
<<Start>>
RegisterSyslogClient
RegisterSyslogClient Completed Successfully.....
<<End>>
```



Note You must reissue this command each time that you stop and start FMMServer on the SPE.



Note See the [“Severity Levels” section on page 1-8](#) for additional information.

Step 6 After performing Step 1 through Step 5, go to the desktop and launch FMMSysLog.exe to begin viewing the FMMSysLog output command level selected. You may need to revise the level by selecting Options from the FMMSysLog menu.



Note Remember to perform these commands only on the SPE running System Manager, because certain FMM services run only on the SPE running System Manager.

FMM Syslog Messages

[Table 2-2](#) lists some of the messages reported by syslog, their meanings, and recommended actions, where applicable.

Table 2-2 FMM Syslog Messages

Message	Meaning	Possible Actions
FMM application cannot communicate with X module (where X is some module within the system).	<ul style="list-style-type: none"> • UPS monitor—If the UPS is monitored through the COM port, the COM port may not be working correctly. If the UPS is monitored through IP, the device is not accessible. • CDP monitor—Cannot get CDP information from the SSP and cannot send CDP information from the SPE to the SSP. • DMI monitor—The Desktop Management Interface (DMI) monitor failed, meaning that there will be no temperature updates for the SPE and no asset information for the SNMP agent. The CPU temperature monitor driver exposes the “DMI String,” representing the CPU temperature. • Hot Swap monitor—Hot-swap functionality is not available. • Alarm Card monitor—No communication with the SAP; no control on the COM ports. • Card Control—No communication with the other cards. • Hardware WatchDog control—If a critical process fails or if the system is not in a stable condition, the system will not reboot immediately. • SPE LED control—The status/alarm LEDs on the SPE cannot be controlled. 	<ul style="list-style-type: none"> • Replace the faulty module, if applicable. • Contact TAC for assistance. See “Contacting the Cisco TAC” on page 2-22.
Module X has restarted successfully (where X is some module in the system).	Some modules, such as the UPS monitor, can recover after a while. When this occurs, a module failure message may be followed by this message.	None.
Hot swap initiated by front panel button.	The SHTDN button on the front panel of a system card has been pressed.	None.

Table 2-2 FMM Syslog Messages (continued)

Message	Meaning	Possible Actions
Process X has failed (where X is some system process).	A process has failed that is started and monitored by the software watchdog. The specific process name is mentioned in the message.	Contact TAC for assistance.
NT system call failure.	An operating system call has failed.	Contact TAC for assistance.
Serial Line Protocol (SLP) user failed to log in. Alarm Card console locked.	The SAP console is locked for SLP commands.	As administrator, try to manually log in to the SAP with a different password, and then reset the SAP password. If this does not work, contact TAC.
FMM application cannot communicate with Alarm Card LED.	The FMM cannot access the SAP LEDs.	Contact TAC for assistance.
SPE rebooting due to process X failure (where X is some system process).	A critical process started and monitored by the watchdog services has failed. As a result, the SPE is rebooting.	Contact TAC for assistance.
FMM process failed to initialize.	The FMM has failed to initialize.	Contact TAC for assistance.
SPE card initialized.	The SPE has initialized.	None.
Alarm card initialized.	The SAP has initialized.	None.
Process X has recovered and restarted (where X is some system process).	The process named in the message, previously started and monitored by the software watchdog, failed but has now restarted.	None.

Using Third-Party Troubleshooting Tools

Third-party diagnostic tools are often the best means of solving difficult problems. For example, invoking a debug command that places heavy demands on system processing power can be disastrous in an environment experiencing excessive traffic. However, attaching a network analyzer to the suspect network is less intrusive and is more likely to yield useful information without interrupting or slowing the operation of the system.

The following are some typical third-party troubleshooting tools:

- [Volt-Ohm Meters, Digital Multimeters, and Cable Testers](#)
- [Time Domain Reflectometers and Optical Time Domain Reflectometers](#)
- [Breakout Boxes, Fox Boxes, Bit Error Rate Testers, and Block Error Rate Testers](#)
- [Network Monitors](#)
- [Network Analyzers](#)

Volt-Ohm Meters, Digital Multimeters, and Cable Testers

Volt-ohm meters and digital multimeters are the simplest cable-testing tools. These devices measure parameters such as AC and DC voltage, current, resistance, capacitance, and cable continuity. They are used to verify physical connectivity.

Cable testers (scanners) also verify physical connectivity. Cable testers are available for shielded twisted pair (STP), unshielded twisted pair (UTP), 10Base-T, and coaxial cables. A cable tester might be able to perform any of the following functions:

- Testing and reporting on cable conditions, including near-end crosstalk (NEXT), attenuation, and noise
- Time domain reflectometer (TDR) functions, traffic monitoring, and wire map functions

Similar testing equipment is available for fiber-optic cable. Fiber-optic cable is expensive and should be tested both before installation (on-the-reel testing) and after installation. Continuity testing of fiber-optic cable requires either a visible light source or an optical time domain reflectometer (OTDR). Light sources

capable of providing light at the three predominant wavelengths (850 nm, 1300 nm, and 1550 nm) are used with power meters that can measure the same wavelengths and that can test attenuation and return loss in the fiber.

Time Domain Reflectometers and Optical Time Domain Reflectometers

TDRs are the most sophisticated cable testers. These devices can quickly locate open and short circuits, crimps, sharp bends, impedance mismatches, and other defects in metallic cables.

A TDR works by bouncing a signal off the end of the cable. Cable opens, cable shorts, and other cable problems reflect the signal back at different amplitudes, depending on the problem. A TDR measures how much time it takes for the signal to be reflected. The TDR then calculates the distance to a fault in the cable. You can also use TDRs to measure the length of a cable. Some TDRs can calculate the propagation rate, based on a configured cable length.

Fiber-optic measurement is performed by an OTDR. OTDRs can accurately measure the length of the fiber, locate cable breaks, measure the fiber attenuation, and measure splice or connector losses. You can use an OTDR to take the “signature” of a particular installation, noting attenuation and splice losses. You can then compare this baseline measurement with future signatures when you suspect a problem in the system.

Breakout Boxes, Fox Boxes, Bit Error Rate Testers, and Block Error Rate Testers

Breakout boxes, fox boxes, bit error rate testers (BERTs), and block error rate testers (BLERTs) are digital interface testing tools used to measure the digital signals present at computers, serial printers, modems, channel service unit/data service units (CSU/DSUs), and other peripheral interfaces. These devices can monitor data line conditions; send, receive, and analyze data; and diagnose problems common to data communication systems. For example, you can examine traffic from data terminal equipment (DTE), such as a computer, through data communications equipment (DCE), such as a modem or CSU/DSU, to help isolate problems, identify bit patterns, and ensure that the proper cabling has been installed. However, you cannot use these devices to test signals passing through Ethernet media.

Network Monitors

Network monitors continuously track packets crossing a network, providing an accurate picture of network activity at any moment or a historical record of network activity over a period of time. Network monitors do not decode the contents of frames.

Monitors are useful for sampling network activity over a period of time to establish a normal performance profile, or *baseline*. Monitors collect information such as packet sizes, number of packets, error packets, overall usage of a connection, number of hosts and the hosts' Media Access Control (MAC) addresses, and details about communications between hosts and other devices. You can use this data to create profiles of LAN traffic and to assist in locating traffic overloads, planning for network expansion, detecting intruders, establishing baseline performance, and distributing traffic more efficiently.

Network Analyzers

A network analyzer (also called a *protocol analyzer*) decodes the various protocol layers in a recorded frame and presents them as readable abbreviations or summaries.

Most network analyzers can perform many of the following functions:

- Displaying information about LAN traffic, providing statistics such as network utilization and packet error rates, and performing limited protocol testing (such as TCP/IP ping tests)
- Filtering traffic that meets certain criteria; for example, all traffic to and from a particular device can be captured
- Time-stamping captured data
- Presenting protocol layers in an easily readable form
- Generating frames and transmitting them to the network
- Incorporating an expert system in which the analyzer uses a set of rules combined with information about the network configuration and operation to diagnose and offer potential solutions to network problems

Contacting the Cisco TAC

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website, at <http://www.cisco.com/tac>.

For additional details on contacting the TAC, see the “[Obtaining Technical Assistance](#)” section in the Preface.

If you cannot resolve your problem using the procedures outlined in this section, collect the following information for your technical support representative:

- ROM images (use the **show version EXEC** command)
- Programmable ROM labels
- NVRAM configurations for system cards
- Debugging output from adjacent Cisco ICS 7750s or Cisco routers, if any, obtained by using the following privileged EXEC commands:
 - **debug ip packet**
 - **debug ip udp**
 - **debug tftp**

For more information about these debug commands, refer to the *Cisco IOS Debug Command Reference*.

