



Monitoring the System

This chapter explains how to monitor the Cisco Integrated Communications System (ICS) 7750 (Cisco ICS 7750). The chapter is organized as follows:

- [Alarms, page 1-2](#)
- [Logging, page 1-4](#)
- [Event Manager, page 1-11](#)
- [SNMP Basics, page 1-18](#)
- [Monitoring with ICS System Manager, page 1-26](#)
- [Monitoring with CiscoWorks2000, page 1-32](#)
- [Monitoring with Cisco IOS Software, page 1-33](#)
- [Monitoring an Uninterruptible Power Supply \(UPS\), page 1-37](#)



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](#).

Alarms

This section describes alarms, which indicate problems on the Cisco ICS 7750 or on systems with which it is communicating.

Alarms are associated with the following faults and event generators:

- Events—Physical occurrences, including chassis-related events, such as temperature abnormalities, fan failures, power supply failures, and degradation, that are detected by the system alarm processor (SAP). The SAP then communicates these events to the Fault Management Module (FMM) running on the system processing engine (SPE) through a serial line. The SPE logs the occurrence in the form of a syslog message.
- Cisco CallManager and FMM—Generate the events related to Cisco CallManager and other applications running on the SPE. Cisco CallManager events generate NT-specific Event Log messages.

Applications running on the SPE, such as Cisco CallManager and Cisco Unity Voice Messaging, are capable of sending syslog messages, but these applications must first be configured to send the messages and must be configured with a destination (the SPE running System Manager).

- Multiservice route processor (MRP)—Trunk cards that house WAN interface cards (WICs), voice interface cards (VICs), and voice WAN interface cards (VWICs) generate traps related to problems such as card failures and configuration changes. Traps are transmitted in the form of Simple Network Management Protocol (SNMP) messages. These messages are received by the Inventory Discovery/Trap Receiver module on the SPE running System Manager for internal use. For each trap, a corresponding syslog message is received by the Event Manager. This syslog message is analyzed against pre-defined rules in FMM. If there is an action specified in FMM for the syslog message, the action is taken. If there is no rule defined in FMM, you can use Event Manager to define specific rules. See the [“Event Manager” section on page 1-11](#).

MRPs also generate syslog messages when specific conditions occur, such as a link-up/link-down state. These syslog messages are received by the CSyslog service on the SPE running System Manager and logged in the syslog database. Each syslog message is analyzed against the rules in FMM. If there is an action specified in FMM for that syslog message, the action is taken (such as setting the alarm LED).

- System switch processor (SSP)—Provides the traps related to the installation or removal of cards in the Cisco ICS 7750 chassis. The behavior of the SSP is similar to the behavior of the MRP.
- Telephony switches—Provide the traps related to the installation or removal of IP phones or other connected network devices.

**Note**

For more information about SNMP messages, see [“SNMP Basics” section on page 1-18](#). To find out how to identify and solve system problems, see [Chapter 2, “System Troubleshooting Guidelines,”](#) and [Appendix A, “Error Message Summary.”](#)

Alarm Notification

The following system components are responsible for issuing notifications of alarms in the following ways:

- FMM is responsible for controlling the state of the LEDs on the system cards, detecting key events, such as chassis faults and MRP card failures, and taking corrective action based on the specific event. For example, if MRP hardware failed to initialize, FMM would set the alarm LED on the MRP card to amber, reflecting a major alarm condition.
- An SNMP agent generates a trap that is collected by ICS System Manager or another SNMP management application, which processes the trap and takes the appropriate action. (SNMP trap processing is limited to internal processing only in ICS System Manager.)
- ICS System Manager collects the syslog messages. It provides the user interface to enable system configuration for specific action to take upon receipt of these syslog messages. ICS System Manager also provides the mechanism to manage syslog messages by configurable options to display the messages, save the messages or report the messages on demand. For example, you can view error messages in the Event Viewer, or you can receive error messages in the form of e-mail or pager alerts, if you have set them up. See [“Event Manager” section on page 1-11](#).
- Through an open communications session with the Cisco ICS 7750, you retrieve log messages associated with alarms.

Alarm Levels

The cards in the Cisco ICS 7750 each have an alarm LED that indicates the status of the hardware and software of that card. The SAP has an alarm LED that indicates the status of the overall system.

Using these alarm LEDs, the system can report the following alarm levels:

- Major alarm (amber LED)—Any state that indicates a system malfunction that can immediately result in a service outage or that indicates a system problem that can seriously degrade service. Examples include the following:
 - System overheating because of high ambient air temperature, an air intake or exhaust blockage, or fan failure
 - A power supply module failure
 - SPE memory parity, disk read/write errors, or network interface card (NIC) failures
 - Digital signal processor (DSP) module failure caused by a fatal error
 - Initialization failures on a T1/E1 driver
- Minor alarm (yellow LED)—Any state that indicates a system abnormality that does not seriously degrade service, but that may affect the network or equipment. Examples include the following:
 - A power supply that has produced an out-of-tolerance output (as when one power supply fails in a chassis with dual power supplies)
 - A port that has become disabled or is otherwise out of service

Logging

This section provides the following information about logging:

- [How to Access Log Messages](#)
- [How to Read Log Messages](#)
- [How to Change the Log Configuration](#)

How to Access Log Messages

You can access log messages in any of the following ways:

- [Handling Log Messages with ICS System Manager](#)
- [Saving Log Messages to a Syslog Server](#)

Handling Log Messages with ICS System Manager

ICS System Manager provides several options for handling the log messages directed to it. By default, the system sends log messages to the SPE, where they are stored on disk.

The FMM module on each SPE running core software is also configured to send FMM syslog messages to ICS System Manager. Syslog messages generated by other applications on the SPE running core software will not be forwarded to ICS System Manager, however, unless you configure the application. If the application is configured to send syslog messages to ICS System Manager, then the messages will be logged in the ICS System Manager syslog database.

Other components in the Cisco ICS 7750 chassis, such as the MRP and SSP, are configured with a syslog destination in the Cisco IOS configuration to send syslog messages to ICS System Manager. This configuration is done through ICSConfig.

**Note**

If you change or delete the syslog destination, ICS System Manager will no longer receive the syslog messages and, therefore, will not be able to react to them.

Saving Log Messages to a Syslog Server

The system saves syslog messages to an internal buffer. You can configure the system to read messages from the buffer and send them to a specified syslog server.

Syslog messages are reported based on severity. The first number following the percent sign (%) in a syslog message indicates the severity of the message. For details, see the [“Severity Levels” section on page 1-8](#).

**Note**

For instructions on how to view and change the log configuration, see [“How to Change the Log Configuration”](#) section on page 1-8.

How to Read Log Messages

When viewed on a log server, the mandatory portion of a log message begins with a percent sign (%) and can contain up to 80 characters. The message fields that precede the percent sign (received and sent dates and times) are optional.

[Table 1-1](#) describes the elements of log messages that can be viewed in Event Manager (see the [“Event Manager”](#) section on page 1-11).

Table 1-1 Log Message Elements

Element	Example	Format	Description
Received date and time	1999 Nov 21 11:55:00	yyyy mmm dd hh:mm:ss	The date and time when the message was received.
Sent date and time	1999 Nov 21 11:55:00	yyyy mmm dd hh:mm:ss	The date and time when the message was sent.
FACILITY	%LPR	STRING	Two or more uppercase letters that indicate the facility to which the message refers (see Table 1-2).
From	192.31.7.19	n.n.n.n	The IP address of the device sending the message.
Message	System temperature OK	string	A description of the event.
CISCO FACILITY (optional)	CDP	STRING	Two or more uppercase letters that indicate the facility to which the message refers. Facilities include hardware devices, protocols, and system software modules.

Table 1-1 Log Message Elements (continued)

Element	Example	Format	Description
CISCO SUBFACILITY (optional)	CIP	STRING	Two or more uppercase letters that indicate the subfacility for Channel Interface Processor (CIP) messages. CIP messages have a Cisco subfacility code of CIP.
Cisco Severity (optional)	1	0–7	A single-digit code from 0 to 7 that indicates the severity of the message (see Table 1-3). The lower the number, the more serious the situation.
CISCO MNEMONIC (optional)	XMIT_ERR	STRING	A code that uniquely identifies the message.

Facilities

[Table 1-2](#) describes the facility types supported by log messages.

Table 1-2 Log Facility Type Keywords

Keyword	Description
auth	Authorization system
cron	Cron facility
daemon	System daemon
kern	Kernel
local0-7	Reserved for user-defined messages (includes local0 through local7)
lpr	Line printer system
mail	Mail system
news	USENET news
syslog	System log
uucp	UNIX-to-UNIX copy system

Severity Levels

Table 1-3 describes log message severity levels.

Table 1-3 Log Message Severity Level Keywords

Keyword	Level	Description	Syslog Definition
emergency	0	System unusable	LOG_EMERG
alert	1	Immediate action required	LOG_ALERT
critical	2	Critical condition	LOG_CRIT
error	3	Error condition	LOG_ERR
warning	4	Warning condition	LOG_WARNING
notification	5	Normal but significant condition	LOG_NOTICE
informational	6	Information—no action required	LOG_INFO
debugging	7	Debugging message	LOG_DEBUG



Note

Not all messages indicate problems. Some messages are informational. Others may help diagnose problems with communications lines, internal hardware, or system software. To find out how to use system messages to identify and solve problems, see [Chapter 2, “System Troubleshooting Guidelines,”](#) and [Appendix A, “Error Message Summary.”](#)

How to Change the Log Configuration

The system sends log messages to ICS System Manager by default. You should not change this default configuration; changing the default configuration may impact the functionality of ICS System Manager. You can, however, add another syslog destination, such as buffers and UNIX hosts that are running a syslog server, to direct these messages.

This section provides the following information about log configurations:

- [Default Log Configuration](#)
- [Configuring the Syslog Daemon on UNIX Syslog Servers](#)
- [Changing Syslog Server Logging](#)

Default Log Configuration

The Cisco IOS components (analog station interface [ASI] cards, MRP cards, and the SSP card) ship with the default logging configuration described in [Table 1-4](#).

Table 1-4 Default Logging Configuration

Configuration Parameters	Default Setting
System message logging to the console	Enabled
System message logging to Telnet sessions	Disabled by no logging monitor command
Log server	Enabled (syslog message is on)
Syslog server IP address	System Manager SPE
Server facility	LOCAL7
Server severity	Warnings (4)
Logging buffer size	500 (Cisco IOS default on MRP/SSP)
Logging history size	1 (Cisco IOS default on MRP/SSP)
Timestamp option	Enabled by service timestamps debug uptime and service timestamps log datetime msec localtime show-timezone commands



Tip

To view the state of syslog error and event logging, including host addresses and whether console logging is enabled, enter the Cisco IOS **show logging** command.

Configuring the Syslog Daemon on UNIX Syslog Servers

Before you can send log messages to a UNIX syslog server, you must configure the syslog daemon on the UNIX server. To configure the syslog daemon, log in as root and include a line such as the following in the file `syslog.conf`:

```
facility.level /syslog_path/myfile.log
```

where

- *facility* is the log facility keyword (see [Table 1-2](#))
- *level* is the severity level (see [Table 1-3](#))
- *syslog_path* is the path to your log file
- *myfile.log* is the name of your log file

The syslog daemon (`syslogd`) sends messages at the level specified in `syslog.conf`, provided that the file exists and provided that `syslogd` has permission to write to it.

Changing Syslog Server Logging

[Table 1-5](#) shows the Cisco IOS commands that can be used in global configuration mode to change syslog server logging behavior. However, the use of the Cisco IOS CLI commands to change the syslog logging host on the Cisco ICS 7750 is prohibited; use `ICSCConfig` instead of the Cisco IOS CLI commands.

Table 1-5 Syslog Server Logging Behavior Commands

Task	Command
Configure a Cisco IOS device to log messages to a syslog server, where <i>host</i> is the name or IP address of the target syslog server.	logging host
Remove a host from the list of syslog servers.	no logging host
Configure a Cisco IOS device to limit the log messages that it sends to the syslog server(s), based on the severity level, where <i>level</i> is one of the log message severity keywords listed in Table 1-3 .	logging trap level
Disable logging to the syslog server(s).	no logging trap

**Note**

Do not use the Cisco IOS CLI commands to change the syslog logging host. Use ICSCConfig for this configuration. See the [“Best Practices for Using the Cisco IOS CLI”](#) section on page 3-43.

**Note**

For more information about the Cisco IOS commands related to logging, refer to the [Configuration Fundamentals Command Reference](#) publication.

Event Manager

ICS System Manager includes an Event Manager that monitors system events. The Event Manager can be configured to invoke action when specific types of events are received. These events are defined by Event Manager rules; the events include conditions, such that when Event Manager receives a system message, that message is compared to the conditions defined in the rules. If the message fulfills the conditions of a rule, then Event Manager will take appropriate action, as defined.

Event Manager enables you to view system events (messages) and to specify how you want the system to respond to a particular type of message. For example, for certain types of log messages, you might want to configure the system to automatically generate an e-mail message or send a page.

To facilitate performance improvements and to provide enhanced support to the Cisco ICS 7500, there is an alert feature in Event Manager which, if enabled, forwards certain performance and availability monitoring event information to the designated system user and to Cisco Systems. SSP, FMM, chassis, and MRP events cause system information to be sent when this feature is enabled.

**Note**

It is strongly recommended that you configure Event Manager to send alerts for system activity. Alerts help to expedite awareness of, and ensure proactive response to, system-related problems.

Enabling or Disabling Availability Notification

The availability notification feature can be enabled or disabled at any time by accessing the Event Manager tab labeled “Availability and Preferences.”

-
- Step 1** From the System Manager home page, click the **Event Manager** tab.
 - Step 2** Click **Availability**.
 - Step 3** Click the **User Consent to Availability** agreement. To enable availability notification, click **Yes, I accept**; to disable availability notification, click **No, I do not accept**.
 - Step 4** Click **Submit**.
-

To set up e-mail alerts, you must consent to the availability agreement displayed on the second page of the ICSCConfig user interface during the initial configuration process. The first screen displays the general license information, and the second page shows the e-mail processing agreement.

Through the Event Manager Preferences page, the following values can be defined:

- Maximum size of the event log that can be viewed
- Default values for event notification through e-mail, message forwarding, and paging
- Choice of system message fields to include in custom reports
- Choice of a field delimiter character for exporting messages to other databases

A description of the fields, links, and controls available through Preferences can be found in the online help section of the Event Manager tab.

Setting E-Mail Notification Defaults

To set e-mail notification, follow these steps:

-
- Step 1** From the System Manager home page, click the **Event Manager** tab.
 - Step 2** Click **Preferences**; the Event Manager Preferences page appears.

- Step 3** In the To field in the E-mail Setting group, enter the default e-mail address to which the e-mail messages should be sent.
 - Step 4** In the From field, enter the default e-mail address from which the e-mail messages originate.
 - Step 5** In the From Name field, enter the default name from which the e-mail messages originate.
 - Step 6** Enter the full e-mail server name in the *servername.maildomain.suffix* format (for example, comail.companyname.com).
 - Step 7** Click **Submit**.
-

Setting and Testing Page Notification Defaults

In addition to e-mail notifications, paging parameters may also be configured to alert you of specific events as they occur on the Cisco ICS 7750. When the paging operation is configured, a numeric page is sent from the Cisco ICS 7750 when condition(s) of a custom rule are met. You must define and create the custom rule that will send a page upon a specific condition. Multiple rules must be created for separate conditions, sending separate pages.

When you create an Event Manager rule that specifies a page operation, you specify a rule condition such as “severity greater than critical.” The page operation requires the page phone number to be specified in the Page To field and the numeric message to be specified in the Numeric Message field in the Page Operation configuration page. (This page phone number will be automatically populated if the Page Setting is entered in the Preferences page.) The numeric message is unique to the condition(s) specified in the rule.

See the ICS System Manager online help for additional information about defining custom rules for use with Event Manager.

To use the paging operation, you must also connect a modem to the console port on the SAP using a serial modem cable (also known as a Data Communications Equipment, or DCE, cable). The US Robotics 56K Fax Modem is recommended, but the paging functionality can be provided by using any modem that can save and restore its settings when the modem is powered on, as long as similar modem settings (as those used on the US Robotics modem) are set.



Note For additional information about installing and configuring the modem, refer to “Initializing a Modem for a SAP” in Chapter 4, “Completing the Cisco ICS 7750 Installation,” in the *Cisco ICS 7750 Installation and Configuration Guide*.

Follow these steps to configure the paging parameters and to test the paging operation on the Cisco ICS 7750:

-
- Step 1** From the System Manager home page, click the **Event Manager** tab.
- Step 2** Click **Preferences**; the Event Manager Preferences page appears.
- Step 3** In the To field in the Page Setting group, enter the pager phone number to which the pages are to be sent, including any Personal Identification Number (PIN) or numeric password that is used for authentication (if required).
- For example, you can define the page setting to include a pager phone number and a PIN or numeric password, such as:
- ```
555-1234,,,,,5678
```
- where *555-1234* is the phone number to which the pages should be sent, the *,,,,,* represents pauses, and *5678* indicates the PIN or numeric password.
- If no PIN or numeric password is required, enter the phone number only (the pauses are not required).
- Step 4** Click **Submit**.
- Test the paging operation to determine successful completion.
- Step 5** Click the **Test Page Setting** button that is located above the To field.
- A popup window appears.
- Step 6** Enter the numeric message that you want to send using the paging operation to determine successful completion.
- For example, if you enter *7750* in the popup window, you should receive a page showing *7750*.
- If the page does not complete successfully, check the Windows 2000 Event Viewer to determine the error messages that were received.
- Step 7** From the Windows Start menu, select **Programs > Administrative Tools > Event Viewer**.
- Step 8** In the left pane, select **Application Log**.

The following error messages originating from the FMMServer and CSyslogd components provide an example of the errors that might be indicated if a modem is not attached to the SAP or if the modem is incorrectly configured:

```
Event Type: Information
Event Source: FMMServer
Event Category: None
Event ID: 0
Date: 10/30/2002
Time: 11:20:15 AM
User: N/A
Computer: VNT4-SPE-CM1
Description:
Modem State changed to DIAL_TIMEOUT
```

```
Event Type: Error
Event Source: CSyslogd
Event Category: None
Event ID: 75
Date: 10/30/2002
Time: 11:20:29 AM
User: N/A
Computer: VNT4-SPE-CM1
Description:
11:20:29.625(4488): SAPageThreadInstance: DialOut() Failed,
hResult = -2147467259 (0x80004005)
```

```
Event Type: Information
Event Source: FMMServer
Event Category: None
Event ID: 0
Date: 10/30/2002
Time: 11:20:29 AM
User: N/A
Computer: VNT4-SPE-CM1
Description:
AlarmCardControl::executeCommand: failed (err=20)
```

**Note**

If you do not receive a page from the Cisco ICS 7750, check to make sure that your modem is connected to the console port on the SAP. If your modem is attached to the COM1 or COM2 port on the SAP, the page will fail.

## Validating E-Mail Settings

To validate and test the e-mail settings on the ICS System Manager Event Manager:

- 
- Step 1** Go to the System Manager web page (<http://xxx.xxx.xxx.xxx/ics>) where *xxx.xxx.xxx.xxx* is the IP address of the SPE running System Manager.
- Step 2** Click the **Event Manager** tab.
- Step 3** Click the **Preferences** link in the left pane.
- Step 4** Complete the E-Mail settings section:
- **To:** E-mail address of the system administrator for the Cisco ICS 7750; this is the default e-mail address to which event notifications will be sent.
  - **From:** E-mail address of the specific Cisco ICS 7750; the default e-mail address showing where event notification e-mails originated. This address appears in the From field of every e-mail message sent from this Cisco ICS 7750. This address should be sufficiently descriptive to uniquely identify the specific system (such as *7750\_xxx@yourcompany.com*, where *xxx* is the last 3 digits of the IP address).
  - **From Name:** From name of the specific Cisco ICS 7750; the default name showing where event notification e-mails originated (should be descriptive).
  - **Email Server:** DNS name of an accessible e-mail server at your site; this must be an e-mail server that the specific Cisco ICS 7750 has security privileges to SMTP-Connect to.
- 

## Testing E-Mail Settings

To test Event Manager e-mail settings, do the following:

- 
- Step 1** Go to the System Manager web page (<http://xxx.xxx.xxx.xxx/ics>) where *xxx.xxx.xxx.xxx* is the IP address of the SPE running System Manager.
- Step 2** Click the **Event Manager** tab.
- Step 3** Click the **Preferences** link in the left pane.

- Step 4** Click the **Test Email Setting** button in the Email Settings title bar; this will send a test e-mail message to the e-mail address specified in the To field via the SMTP e-mail server specified in the Email Server field.
- 

If you do not receive an alert notification from the Cisco ICS 7750, it is possible that the following conditions occurred:

- No availability e-mail was triggered.
- Incorrect e-mail settings were defined.
- Correct e-mail settings were defined, but the Cisco ICS 7750 is inside a secure network, or is behind a firewall, with no access to the specified e-mail server.
- An e-mail account was not set up.
- Incorrect DNS entries were defined.
- If you are using the paging function, your modem might be attached to the COM1 or COM2 port on the SAP; it must be connected to the console port on the SAP.

## Additional Verification of Correct E-Mail Settings

If you completed the steps in the “[Testing E-Mail Settings](#)” section on page 1-16 but did not receive a test e-mail within 10 minutes, follow these steps to log into the Event Viewer and verify the accuracy of the e-mail settings:

---

- Step 1** Use Terminal Services Client to access the Cisco ICS 7750.
- Step 2** From the Windows Start menu, select **Programs > Administrative Tools > Event Viewer**.
- Step 3** In the left pane, select **Application Log**.
- Step 4** Look for an entry with the source name CSyslogd, and double-click it (the service that sends SMTP e-mail messages for the Cisco ICS 7750 is the Cisco Syslog daemon).

If the SMTP e-mail client software is having difficulty connecting to the e-mail server specified in the Event Manager e-mail settings, CSyslogd will log an error to the Event Viewer log.

---

If a change has been made to the location to which alerts are to be sent, but the notifications are still going to the previously defined location, do the following:

- Check to see whether e-mail rules were created. If rules were created, check to verify that the To field in the rule is empty (so the rule will use the Preferences setting). You can see custom rules in the Event Manager screen.
- Restart the CSyslogd service from Services on the SPE running System Manager by choosing **Start > Programs > Administrative Tools > Services**. Right-click the CSyslogd service, and click **Stop**. After the service has stopped, click **Start**. A message will appear that asks whether you wish to restart two other (dependent) services also; reply “yes.” This is a nondestructive restart and will force the CSyslogd service to get the correct information from the SQL database tables.

If you can see the correct information in the System Manager Event Manager Preferences GUI, the correct information is in the SQL table. This would indicate that the CSyslogd service was not correctly notified that the Preferences information had changed or that an error occurred when CSyslogd attempted to reread the information from the SQL table. The remedy described in this section should resolve the problem.

## SNMP Basics

SNMP facilitates the exchange of management information among network devices. SNMP is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables you to manage network performance, find and solve network problems, and plan for network growth.

## SNMP Components

An SNMP-managed network consists of three key components: managed devices, agents, and network management systems (NMSs).

- A managed device is a network node that contains an SNMP agent and resides on a managed network. Managed devices collect and store management information and make it available using SNMP. The Cisco ICS 7750 includes the following managed devices:
  - System processing engine (SPE) cards
  - Analog station interface (ASI) cards
  - Multiservice route processor (MRP) cards
  - System switch processor (SSP) card
- An agent is network-management software that resides on a managed device. An agent has local knowledge of management information and translates it into a form compatible with SNMP. The agent on the Cisco ICS 7750 is located on the SPE running System Manager.

In the Cisco ICS 7750 chassis, each system card runs its own SNMP agent. The SPEs run the Microsoft SNMP agent; the SPE running System Manager also runs its own proxy agent in addition to the Microsoft SNMP agent. The proxy agent runs on the default port (port 161), while the Microsoft SNMP agent runs on a different port.

The individual agents on each system card can be queried directly by the SNMP agent, or they can be queried through the ICS System Manager proxy agent by appending the slot number to the community string.

For example, to access the Management Information Bases (MIBs) from the card in slot 5, you can direct the request to the SPE running System Manager with the following community string:

```
public@Slot5
```

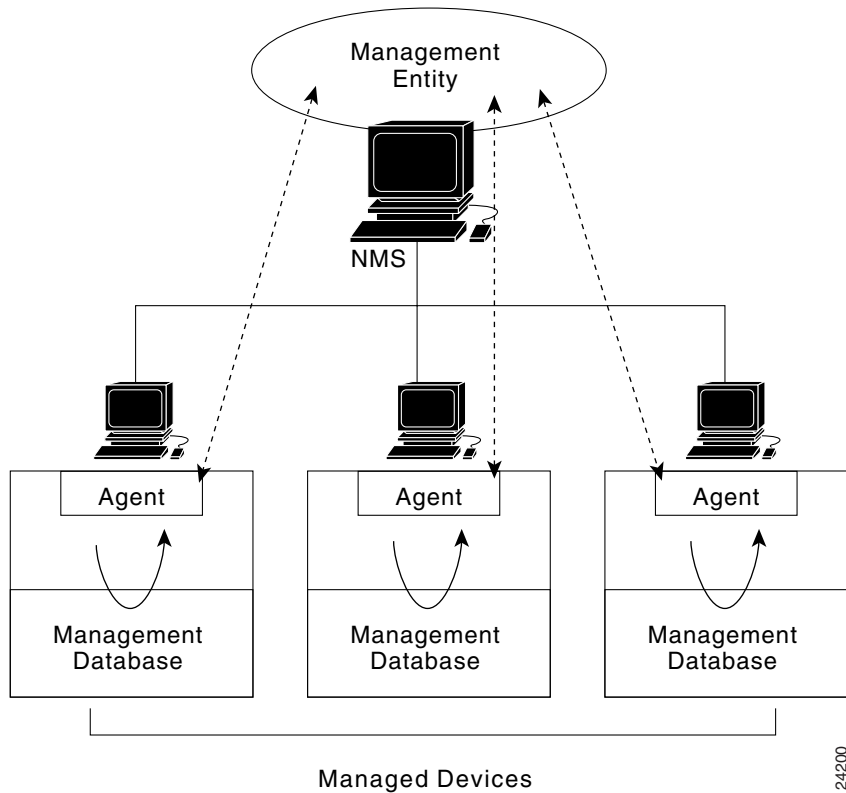
See the “[SNMP Management Information Base](#)” section on page 1-21 for additional information about MIBs. See the “[Understanding Community Strings](#)” section on page 1-25 for additional information about community strings.

- An SNMP management application, together with the computer it runs on, is called a *network management system* (NMS). An NMS executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. The Cisco ICS 7750 is compatible with the following NMSs:
  - ICS System Manager
  - CiscoWorks2000

- HP OpenView

Figure 1-1 shows the relationships among the managed devices and agents and the NMS.

**Figure 1-1 Major Components of SNMP-Managed Networks**



The following system components, though not SNMP-managed devices, receive SNMP support through ICS System Manager:

- SAP card
- Power supply modules
- Fans
- Chassis

## SNMP Management Information Base

A Management Information Base (MIB) is a collection of information that is organized hierarchically. MIBs are accessed by using a network management protocol such as SNMP. They comprise managed objects, which are identified by object identifiers.

A managed object (sometimes called a *MIB object* or an *object*) is one of any number of specific characteristics of a managed device. Managed objects comprise one or more object instances, which are essentially variables.

## Using SNMP with MIB Variables

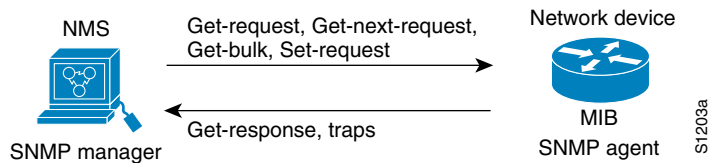
System MIB variables are accessible through SNMP as follows:

- Accessing a MIB variable—This function is initiated by the SNMP agent in response to a request from the NMS. The agent retrieves the value of the requested MIB variable and responds to the NMS with that value.
- Setting a MIB variable—This function is also initiated by the SNMP agent in response to a message from the NMS. The SNMP agent changes the value of the MIB variable to the value requested by the NMS.

Instead of defining a large set of commands, SNMP places all operations in *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 in that SNMP agent.

On the Cisco ICS 7750, the ICS System Manager software (the NMS) typically sends SNMP requests to a single IP address to access the SNMP MIBs of any system component. The SNMP agent can then respond to MIB-related queries sent by the NMS. Similarly, if CiscoWorks2000 is the NMS, it uses the MIB variables to set device variables and to poll devices on the network. You can then display the data that CiscoWorks2000 collects as a graph and analyze it to enhance network performance, to monitor traffic loads, or to troubleshoot problems. (See [“Monitoring with CiscoWorks2000” section on page 1-32.](#))

As [Figure 1-2](#) shows, 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 (see [“Understanding Traps” section on page 1-24](#)) to the manager.

**Figure 1-2** SNMP Network

The SNMP manager uses information in the MIB to perform the operations described in [Table 1-6](#).

**Table 1-6** 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.                                                                                                                    |
| get-response     | The reply to a get-request, get-next-request, and set-request sent by an NMS.                                                                                        |
| get-bulk         | (SNMP version 2 only.) Retrieve large blocks of data, such as multiple rows in a table, which would otherwise require the transmission of many small blocks of data. |
| set-request      | Stores a value in a specific variable.                                                                                                                               |
| trap             | An unsolicited message sent by an SNMP manager, which indicates that some event has occurred.                                                                        |

## Supported MIBs

The Cisco ICS 7750 supports the following MIBs:

- CISCO-C2900-MIB—Supports the SSP card.
- CISCO-ICSUDSU-MIB—Supports integrated channel service unit/data service unit (CSU/DSU) interfaces in the MRP.
- CISCO-VOICE-IF-MIB—Supports ISDN and analog interfaces in the MRP.
- CISCO-ENTITY-FRU-CONTROL-MIB—Supports field-replaceable units (FRUs), such as cards, power supply modules, and the fan tray.
- ENTITY-MIB—Supports the chassis.

- MIB II (RFC1213)—Represents Ethernet and other types of addresses.
- DS1 MIB (RFC1406)—Represents DS1 interfaces in the MRP.

The supported MIBs, by individual system card, are as follows:

- All SPEs:
  - RFC1213 (SYSTEM group)
  - HOST-RESOURCE-MIB
  - CISCO-CDP-MIB
- SPE running System Manager (additional support beyond all SPEs):
  - ENTITY-MIB
  - CISCO-ENTITY-FRU-CONTROL-MIB
  - CISCO-ASSET-MIB
- MRP:
  - RFC1213
  - CISCO-ICS-DSU-MIB
  - OLD-CISCO-CHASSIS-MIB
  - RFC-1406
  - CISCO-CONFIG-MAN-MIB
  - OLD-CISCO-SYS-MIB
  - CISCO-ISDN-IF-MIB
  - RFC1315-MIB
  - RFC1382-MIB
  - CISCO-VOICE-ANALOG-IF-MIB
  - OLD-CISCO-INTERFACES-MIB
  - RFC1398-MIB
  - CISCO-ISDNu-IF-MIB
- SSP (all the MIBs supported in the Catalyst 2900XL switch are available for the SSP):
  - RFC1213
  - CAT2900XL-MIB

- CLUSTER-MIB
- STACK-MAKER-MIB

## Understanding Traps

An agent can send traps to the manager that identify important system events. The following are examples of situations in which an agent might send an SNMP trap message to an NMS specified as a trap receiver:

- An interface or card starts or stops running.
- Spanning-tree topology changes are made.
- Authentication failures occur.

When an agent detects an alarm condition, it reacts by logging information about the time, type, and severity of the condition and generates a trap—or notification message—that is sent to certain IP addresses.

## Cisco ICS 7750 Traps

Cisco ICS 7750 ASI cards, MRP cards, and the SSP card can generate traps such as the following:

- `coldStart`—Indicates power-up reset of a card.
- `warmStart`—Indicates that software running on a card has been upgraded or that the card has been reset.
- `linkDown`—Indicates that a port changed to a suspended or disabled state because of a secure address violation (mismatch or duplication), a network connection error (such as a loss of Link Beat or a jabber error), or an explicit management disable action.
- `linkUp`—Indicates that a port has changed from a suspended or disabled state to the enabled state.
- `authenticationFailure`—Indicates that an SNMP message has been received that is not properly authenticated; that is, the message is not accompanied by a valid community string.

- `addressViolation`—Indicates that an address violation has been detected on a secured port.
- `broadcastStorm`—Indicates that the number of broadcast packets received in a second from a port is higher than the broadcast threshold.

## Understanding Community Strings

SNMP *community strings* authenticate access to MIB objects and function as embedded passwords.

The Cisco ICS 7750 uses a base community string, to which the string `@SLOTnumber` can be appended to form a *composite community string*:

*base community string*@SLOTnumber

where

- *Base community string* represents the get or set community string. For get (read-only) requests, the community string, or password, has a default ASCII value of *public*. For set (read-write) requests, the community string has a default value of *changeme*.
- *Number* represents the target physical slot number (slot 0 through slot 6) of the SNMP request. (This number uses a 0-based slot index, so physical slot 1 in the chassis is designated as slot 0.) The SAP, which is physically installed in slot 8, does not have an SNMP agent.



### Note

The valid community strings are `@SLOT0` through `@SLOT6`. The proxy agent in the SPE running System Manager will forward the SNMP request to the card in the specified slot. Specifying any other slots, such as `@SLOT7` or higher, will result in an invalid community string, as will specifying a slot that does not contain a card.

The SNMP community strings configured for the SNMP service must be synchronized with the ICS System Manager database. This service synchronization is accomplished by configuring the SNMP settings only through ICSCfg.

For example, if a particular SNMP request needs to reach an MRP card in slot 3, the following composite community string could be used:

```
ICS7750@SLOT3
```

where *ICS7750* represents the standard system get (*public*) or set (*changeme*) community string.

## Modifying the Base Community String

You can use ICS System Manager to modify the default read-only and read-write community strings. (Refer to the ICS System Manager online help.)

# Monitoring with ICS System Manager

ICS System Manager monitors the Cisco ICS 7750 device information through the Monitor applet. Monitor provides information such as the following:

- ASIs and MRPs—ICS System Manager provides information about trunk errors, interface errors, memory usage, buffer failures, buffer creation, and ASI and MRP usage.
- SSP—ICS System Manager provides information about SNMP, IP, Internet Control Message Protocol (ICMP), TCP and User Datagram Protocol (UDP) errors, as well as information about SSP usage.

From the SPE running System Manager, use the Monitor tab to access the Monitor page. The Monitor page lets you view current data about the Cisco ICS 7750, by system card, such as the CPU usage and disk space available on your SPE, or the line protocol status and number of inbound and outbound packets transferred over a Fast Ethernet port on the SSP.

The Monitor page consists of three frames: the [Inventory Tree](#), the [Monitorable Fields List](#), and the [Monitored Fields List](#). These frames can be resized by clicking and dragging the borders between the frames.

You can configure the Monitor page to monitor specific Cisco ICS 7750 system cards, which are organized into a hierarchical tree called the [Inventory Tree](#). The Inventory Tree shows each slot in your Cisco ICS 7750 and the system cards that populate each slot. The Monitor applet uses SNMP MIB queries to retrieve the requested information.

Each system card has various associated inventory items. These inventory items are specific pieces of hardware, such as an Ethernet port, or specific file systems, such as the Windows 2000 system.

Each system card and inventory item has various associated fields. Each field represents one monitorable piece of data.

**Note**

---

Refer to the ICS System Manager online help for additional information on configuring and using Monitor.

---

## Inventory Tree

The Inventory Tree depicts the Cisco ICS 7750 as a hierarchical tree.

The top, or root, level indicates the active SPE that is connected to the browser. This is represented by the system host name at the top of the tree. The next level of the tree depicts the system cards, and the third level of the tree depicts the inventory items associated with each system card.

To display the inventory items associated with a system card, click the triangle next to the system card. The triangle points down, indicating that the items associated with that system card are shown.

**Note**

---

You can display the inventory items for only one system card at a time.

---

To select a system card or inventory item, click it. The fields associated with the selected system card or inventory item appear in the [Monitorable Fields List](#).

The Inventory Tree has a popup menu that you can activate by right-clicking anywhere within the frame. The popup menu has the following functions:

- **Reload Inventory**—This option causes the fields and values in all three frames to refresh. All system cards are rediscovered, all fields associated with the selected card or inventory item are listed again in the Fields List, and all field values shown in the [Monitored Fields List](#) are updated with current values.
- **Help**—Displays this help page.

## Monitorable Fields List

The Monitorable Fields List displays all the data fields associated with a system card or inventory item selected in the [Inventory Tree](#). Each field represents one monitorable piece of data related to the selected inventory item. The name of the system card or inventory item to which these fields are associated is indicated by the item selected in the Inventory Tree.

To monitor a field, double-click it. Selected fields appear in bold in the [Monitored Fields List](#), which displays the value of the field. You can select and monitor any number of fields.

**Note**

---

You can select multiple fields by holding down the **Ctrl** key and clicking individual fields, or by holding down the **Shift** key and clicking the first and last field in a series that you want selected.

---

The Fields List contains the following two buttons:

- **Add**—Adds the selected field(s) to the Monitored Fields List, displaying the current value of the field(s).
- **Properties**—Displays the Field Properties dialog box for the highlighted field.

The Fields List has a popup menu that you can activate by right-clicking anywhere within the frame. The popup menu has the following items:

- **Add**—Adds the selected field to the [Monitored Fields List](#), displaying the current value of the field. Because the data is polled, field values are automatically updated based on the field's polling interval.
- **Add All**—Automatically selects and adds all the fields associated with the selected system card or inventory item to the [Monitored Fields List](#).
- **Show All Fields**—When this option is selected, all fields associated with a selected system card or inventory item appear in the [Monitorable Fields List](#). This option is selected by default. When this option is not selected, all of the fields are not displayed.
- **Auto-Select Common Fields**—When this option is selected, fields that are commonly viewed are automatically selected and added to the Monitored Fields List when the associated system card or inventory item is selected. This option is deselected by default.

- **Field Properties...**—Displays the Field Properties Dialog Box for the field currently highlighted.
- **Help**—Displays this help page.

## Monitored Fields List

The Monitored Fields List displays the values of the fields that have been selected for monitoring.

Each row in the list represents one field. There are two columns:

- The **Field Name** column displays the full name of the field, including the system card or inventory item to which the field is associated and a check box. When the check box is selected, the field value is updated automatically at regular intervals as determined in the Field Properties dialog box. When deselected, the field is updated only when you choose to refresh the field values.
- The **Field Value** column shows the current value of the field. Note that different fields display different types of data. Most fields display a numerical or text value, but some display a Boolean yes/no value, and others show a graphical representation.

The Monitored Fields List includes the following buttons:

- **Remove**—Removes the selected field(s) from the Monitored Fields List.
- **Update Now**—Refreshes the selected field(s), displaying the current value of the field(s).
- **Chart**—Displays the Chart dialog box for the selected field.
- **Properties**—Displays the Field Properties dialog box for the selected field.

The Monitored Fields List has a popup menu that you can activate by right-clicking one of the fields listed. The popup menu has the following options:

- **Active**—When enabled, this option causes the selected field(s) to be automatically updated at intervals determined in the Field Properties dialog box.
- **Update Now**—This option causes the selected fields to immediately refresh and display the current field value.
- **Remove Field**—Removes the selected field(s) from the Monitored Fields List.

- Chart...—Displays the Chart dialog box for the selected field.
- Field Properties...—Displays the Field Properties dialog box for the selected field.
- Use Short Field Names—When enabled, this option causes the Field Name columns to show just the field names and to hide the system card or inventory item names. When disabled, the Field Name column also shows the system card and inventory item names. Because you can add fields from more than one item at a time to this list, and because field names may be the same for different items, this option is disabled by default.
- Help—Displays this help page.

## Setting Monitor Polling

Monitor fields can be automatically updated at various intervals or can be set to update only when an update is manually specified. When a field is initially added to the [Monitored Fields List](#), it defaults to the automatic update rate specific to the field. The default automatic date rate varies for each field and can range from 10 to 60 seconds.

Follow these steps to change the update status for a field:

- 
- Step 1** Right-click the field in the [Monitored Fields List](#). The Monitor popup menu appears.
- Step 2** The Active option on the popup menu indicates whether automatic polling is enabled. To toggle automatic polling on or off, select or deselect the Active check box in the popup menu.
- 

Follow these steps to change the frequency that a field is automatically updated:

- 
- Step 1** Click the field in the [Monitored Fields List](#) to select it.
- Step 2** Click **Properties**.  
The Field Properties Dialog Box appears.

- Step 3** In the Polling Interval field, enter the number of seconds that you want to elapse before the field value is automatically updated.
- Step 4** Click **OK**.
- 

## Viewing Current System Data

All viewable data about your Cisco ICS 7750 is arranged logically into lists of fields, with each field representing one piece of data. For example, to view the number of octets sent out over a Fast Ethernet interface on the SSP, you would view the Outbound Octets field that is associated with that particular interface.

To select fields and view current system data:

- 
- Step 1** From the ICS System Manager main page, click **Monitor**.
- Step 2** In the [Inventory Tree](#), click the system card that contains the inventory item you want to view. All inventory items associated with that system card are shown.
- Step 3** Select the system card or inventory item you want to view. The [Monitorable Fields List](#) displays the fields associated with that item.
- Step 4** In the Fields List, select the name of the field that you want to view. To select the field, double-click it, select it, and click **Add**. Or right-click and select **Add** from the popup menu. The field will appear on the [Monitored Fields List](#).



**Note** You can select multiple fields by holding down the **Ctrl** key and clicking individual fields, or by holding down the **Shift** key and clicking the first and last field in a range that you want to select.

---

The selected fields and the current values of those fields are displayed in the Monitored Fields List.

---

**Note**

For information about monitoring individual Cisco IP Phones or the lines connecting those devices to the Cisco ICS 7750, refer to the *Cisco CallManager Serviceability Administration Guide*. For additional information about monitoring the system with ICS System Manager, refer to the ICS System Manager online help.

## Monitoring with CiscoWorks2000

CiscoWorks2000 uses SNMP to monitor and control system devices. You can integrate CiscoWorks2000 applications with other NMSs, such as HP OpenView.

### CiscoWorks2000 Applications

CiscoWorks2000 applications extend industry-standard network management systems to facilitate the following activities:

- Checking the status of Cisco devices
- Maintaining device configurations and inventories
- Troubleshooting device problems.

The CiscoWorks2000 applications for monitoring the SNMP devices on your network include the following:

- Path Tool—Graphically displays a 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 that might be operating in a degraded mode and displays them in a graph.
- Show Commands—Displays data similar to output from the Cisco IOS **show** commands.
- Health Monitor—Provides device status and access to several CiscoWorks2000 applications in one window (including Show Commands and Real-Time Graphs) to monitor 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 devices on the network.

## Using CiscoWorks2000 for Network Management

CiscoWorks2000 runs an AutoDiscovery mechanism to discover the entire network, of which Cisco CallManager may be one component. Since Cisco CallManager supports Cisco Discovery Protocol (CDP), CiscoWorks2000 can also identify the SPE on which Cisco CallManager is running as a Cisco CallManager device.

### SNMP and the CiscoWorks2000 Interface

Using SNMP, CiscoWorks2000 retrieves CDP information by polling Cisco CallManager. After the discovery process is completed, a topology map is generated that identifies all the Cisco CallManager installations in the network.

CiscoWorks2000 also polls other MIB tables in the CISCO-CCM-MIB to gather information required by other components, such as User Tracking (refer to the CiscoWorks2000 Campus Manager online documentation). CiscoWorks2000 periodically polls these agents to obtain additional updated information.

**Note**

---

For examples of how to use CiscoWorks2000 to troubleshoot network problems, see [Chapter 2, “System Troubleshooting Guidelines.”](#)

---

## Monitoring with Cisco IOS Software

This section describes proven strategies to help you monitor your network.

## Evaluating System Performance

Collecting, analyzing, and archiving system performance data is important in understanding how well your system is meeting your organization's needs. Important things to monitor are the behavior of network applications and protocols and the response time of individual devices, such as MRP cards and Catalyst 3524-PWR XL switches.

Common ways to monitor system performance include the following:

- [Evaluating Reachability and Response Times](#)
- [Evaluating Traffic Loads](#)

### Evaluating Reachability and Response Times

Polling remote parts of the network enables you to test reachability and to measure response times. Response-time measurements are made by sending a ping (packet internet groper) packet and measuring the round-trip time (RTT) that it takes to send the packet and receive a response. The ping packet is sent and received as an ICMP echo packet.

**Note**

---

For information about **ping** command usage, see [Chapter 2, “System Troubleshooting Guidelines,”](#) and [Chapter 6, “Solving Serial Connection Problems.”](#)

---

**Caution**

---

Polling activity can result in a significant increase in network traffic. Therefore, it is important to carefully assess what level of monitoring is appropriate for your organization.

---

### Evaluating Traffic Loads

You can use protocol analyzers or SNMP tools to record traffic loads between important sources and destinations. (See [Chapter 2, “System Troubleshooting Guidelines,”](#) for additional information about protocol analyzers and other monitoring and troubleshooting tools.) The objective is to document how much data can pass between pairs of autonomous systems, networks, hosts, or applications.

Source and destination traffic-load documentation is useful for capacity planning and troubleshooting. Source and destination traffic-load data is also useful if you have a service-level agreement that includes throughput requirements.

## In-Band Versus Out-of-Band Monitoring

Another important factor affecting performance of network monitoring is the degree to which monitoring consumes system bandwidth. Depending on how your network is structured, you can use in-band monitoring, out-of-band monitoring, or a combination of the two.

With in-band monitoring, network management data is sent over the same paths as user traffic. This means that any problems on the network will be more difficult to solve because collecting troubleshooting data will take longer. Using management tools is beneficial even when the internetwork is congested, failing, or under a security attack.

With out-of-band monitoring, network management data travels on different paths than user data. NMSs and agents are linked by circuits that are separate from the internetwork. The circuits can use dial-up, ISDN, or other technologies. The separate circuits can be used all the time, or they can be used as backup only when the primary internetwork path is broken.

## Using show Commands

You can use the Cisco IOS **show** commands to perform a variety of tasks:

- Monitor behavior during installation
- Monitor normal network operation
- Isolate problem interfaces, nodes, media, or applications
- Determine when a network is congested
- Determine the status of servers, clients, or other neighbors

## Common show Commands

Commands that you are likely to use include the following:

- The **show interfaces** command displays statistics for network interfaces. (For example, **show interfaces serial** and **show interfaces ethernet**.)
- The **show buffers** command displays statistics for the buffer pools on the target device.
- The **show memory** command shows statistics about the device's memory.
- The **show processes** command displays information about the active processes on the device.
- The **show stacks** command displays information about the stack utilization of processes and interrupt routines, as well as the reason for the last system reboot.
- The **show version** command displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

## Searching and Filtering Output of show Commands

In Cisco IOS Release 12.0(1)T or later, you can search and filter the output for **show** commands. This functionality is useful when you need to sort through large amounts of output, or if you want to exclude output that you do not need to see.

To use this functionality, enter a **show** command followed by the “pipe” character (`|`), one of the keywords **begin**, **include**, or **exclude**, and an expression that you want to search or filter on:

```
command | {begin | include | exclude} regular-expression
```

The following is an example of a **show interface** command that provides information only about lines in which the word “protocol” appears:

```
Cisco ICS 7750# show interface | include protocol
FastEthernet0/0 is up, line protocol is up
Serial4/0 is up, line protocol is up
Serial4/1 is up, line protocol is up
Serial4/2 is administratively down, line protocol is down
Serial4/3 is administratively down, line protocol is down
```

For more information on search and filter functionality, refer to the “Basic Command-Line Interface Commands” section in the “Cisco IOS User Interfaces Commands” chapter in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

# Monitoring an Uninterruptible Power Supply (UPS)

This section explains how to monitor an APC Smart-UPS.

## Connecting and Powering Up the UPS Components

Complete the following steps to set up the components:

- 
- Step 1** Connect the UPS to the SAP card COM1 port or to an Ethernet switch that is connected to the Cisco ICS 7750.
- Step 2** If any of the following devices are not turned on, power them on as follows:
- UPS—Press the Test button on the UPS front panel.
  - Cisco ICS 7750—Press the power supply switches (on the right side of the chassis) to on ( I ).
  - Catalyst switches—Connect one end of the AC power cord to the AC power connector on the switch; then connect the other end of the power cord to an AC power outlet.
- Step 3** Complete the procedure that is appropriate for the type of UPS connection that you made in Step 1:
- SAP Card COM1 Port—Go to the [“Configuring the System to Monitor the UPS Through a Serial Connection”](#) section on page 1-38.
  - Ethernet switch—Go to the [“Configuring the System to Monitor a UPS Through an Ethernet Connection”](#) section on page 1-39.
-

## Configuring the System to Monitor the UPS Through a Serial Connection

If the UPS serial port is connected to the SAP card COM1 port on the Cisco ICS 7750, complete the following steps to configure the UPS so that the Cisco ICS 7750 can monitor UPS status:

- 
- 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*).



---

**Note** This UPS installation procedure has not been tested with a CD-ROM drive attached to the SPE.

---

- Step 3** Enter the following command to stop the FmmServer on the SPE running System Manager:

```
net stop FmmServer
```

- Step 4** Change to the FMM directory:

```
cd Program Files\Cisco Systems\ics\FMM
```

- Step 5** Install the UPS:

```
installups
```

- Step 6** Start FmmServer:

```
net start FmmServer
```

Go to the [“Verifying That the Cisco ICS 7750 Can Communicate with the UPS”](#) section on page 1-42.

---

# Configuring the System to Monitor a UPS Through an Ethernet Connection

If the UPS is connected to an Ethernet switch that is connected to the SSP card on the Cisco ICS 7750, complete the following steps to configure the UPS so that the Cisco ICS 7750 can monitor UPS status:

---

**Step 1** Ensure that you have the following information available:

- The IP address that you intend to use for the UPS
- The IP address of the SPE configured to monitor the UPS

**Note**

Either the SPE running System Manager or an SPE running core software can be configured to monitor the UPS.

---

- The subnet mask that you used when you configured the Cisco ICS 7750

**Step 2** Insert the Web/SNMP Management CD-ROM that came with your APC Smart-UPS into your PC CD-ROM drive.

**Step 3** Follow the on-screen prompts to install the SNMP/Web Management Utility.

**Note**

If the SNMP/Web Card Management Wizard does not automatically run after the software installation is complete, click **Start > Programs > APC Card Management Wizard**.

---

While the system is attempting to communicate with the UPS, the first screen of the Web/SNMP Management Wizard continues to be displayed (this process might take several minutes). When the system is ready for you to continue with configuring the UPS, the Found An Unconfigured Management Card dialog box appears.

**Step 4** Enter the following information in the Found An Unconfigured Management Card dialog box:

- In the System IP Address field, enter the UPS IP address.
- In the Subnet Mask field, enter the Cisco ICS 7750 subnet mask.

- In the Default Gateway field, enter the IP address of the default gateway.
- Check the **Start a Web browser when finished** check box.

**Step 5** Click **Finish**.

A dialog box appears, which informs you that your default Web browser will start and that your User Name and password for the UPS configuration will be *apc*.

**Step 6** Click **OK**.

**Step 7** Click **Next**.

**Step 8** In the Installation Options dialog box, choose **Express**.

**Step 9** Click **Next**.

**Step 10** Choose the type of connection (LAN) that you are using to communicate with the UPS.

**Step 11** Click **Next**.

**Step 12** Click **Close**.

**Step 13** Click **OK**.

**Step 14** If a Web browser (Netscape Communicator or Microsoft Internet Explorer, for example) is not already running, open it. In the Location or Address field of the browser, enter your UPS IP address.

The Username and Password Required dialog box appears.

**Step 15** In the User Name and Password fields, enter **apc**.

**Step 16** Click **OK**.

The APC Status Summary page appears in your browser.

**Step 17** In the left pane of the browser window, choose **Smart-UPS 1400 RM XL > PowerChute**.

**Step 18** In the Add Client IP Address field, enter the IP address of the SPE running System Manager.

**Step 19** Click **Add**.

The IP address that you entered in Step 18 will appear in the Configured Client IP Addresses pane.

**Step 20** In the left pane of the browser window, choose **Network > SNMP**.

**Step 21** In the SNMP table, verify that the Access field is set to **enabled**.

**Step 22** Click **Apply**.

- Step 23** In the Trap Receiver table, enter the UPS IP address in the Public field.
- Step 24** Click **Apply**.
- Step 25** In the Access Control table, enter the UPS IP address in the Private and Public fields.
- Step 26** Click **Apply**.
- Step 27** In the left pane of the browser window, choose **Event Log**.  
The UPS reports its status in the Event column. Text similar to the following will be displayed:  
Management Card: Web User apc logged in from <IP address>
- Step 28** Unplug the UPS power cord.  
The UPS emits an audio tone.
- Step 29** Plug the UPS power cord in again.  
In the Event column of the Event Log, text similar to the following will be displayed.  
UPS: Switched to battery backup power, utility power failure.  
UPS: Returned from battery backup power, utility power restored.
- Step 30** 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 31** Log in as an administrator (userID *administrator*), and enter your password (the default is *changeme*).
- Step 32** Enter the following command to stop the FMMServer on the SPE running System Manager:  
`net stop FmmServer`
- Step 33** Change to the FMM directory:  
`cd Program Files\Cisco Systems\ics\FMM`
- Step 34** Install the UPS:  
`installups`

**Step 35** Start FMMServer:

```
net start FmmServer
```

**Step 36** Using the FMMcli application program interface, set the host name of the UPS, where *Name* is the IP address of the UPS:

```
FMMcli SetUPSHostName -HostName Name
```

Continue with the [“Verifying That the Cisco ICS 7750 Can Communicate with the UPS” section on page 1-42](#).

---

## Verifying That the Cisco ICS 7750 Can Communicate with the UPS

Complete the following steps to verify that the Cisco ICS 7750 can communicate with the UPS:

- 
- 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** Change to the FMM directory on the SPE:

```
cd Program Files\Cisco Systems\ics\FMM
```

- Step 4** Verify that the Cisco ICS 7750 can communicate with the UPS by executing the following command on the SPE that is configured to monitor the UPS:

```
FMMcli getchasisinfo | more
```

Information similar to the following will be displayed:

```
UPS status = AC
Battery Level = <non-zero value>
Batt. Span = <non-zero value>
```



---

**Note** If *UPS status = UpsNotAvailable* is displayed, verify that your system components are properly connected and powered on. Then try this procedure again.

---

**Step 5** Unplug the UPS power cord.

The UPS emits an audio tone, and the ALARM LED on the SAP turns on (amber).

**Step 6** Enter the following command to verify that the system has detected the change in power status:

```
FMMLi getchasisinfo | more
```

Information similar to the following will be displayed:

```
UPS status = DC
Batt. Level = <non-zero value>
Batt. Span = <non-zero value>
```

**Step 7** Open an ICS System Manager session.

**Step 8** Click the **Event Manager** tab on the ICS System Manager home page.

**Step 9** At the bottom of the Live Viewer page, click **Start Events**.

Information similar to the following will be displayed:

```
AC power is off, using DC
```

---

