Chapter3
Fault Management

This chapter describes the CiscoWorks fault management features that help you monitor and diagnose your network problems. This includes diagnosing individual devices, lines, and interfaces, detecting potential faults, and recovering from problems.Use the following features to perform fault management:

- Troubleshooting scenarios to help you identify the appropriate CiscoWorks application to use to resolve your network problems
- Device Monitor to monitor your network devices
- Environmental Monitor to monitor your network device environment
- Path Tool to locate your device routing paths
- Real-Time Graphs to graph your real-time device data
- Show Commands to view router data
- Health Monitor to query your device health
- Device contact information to troubleshoot network problems
- Log Manager as a diagnostic tool

Fault Management Applications

Several CiscoWorks applications help monitor and diagnose the SNMP devices in your network. Use the following CiscoWorks applications when performing fault management. A brief description of each application follows.

- Device Monitor—Monitors specific devices for environmental and interface information. Sends event information to SunNet Manager (SNM) that causes a glyph to change state.
- Path Tool—Graphically displays a route of the path from a source device to a destination device.

- Environmental Monitor—Graphically displays the temperature and voltage data from an AGS+ router.
- Real-Time Graphs—Monitors the behavior of device interfaces or other network elements suspected of operating in a degraded mode and displays them in a graph.
- Show Commands—View data similar to output from router EXEC **show** commands.
- Health Monitor—Provides information about the health of a device with access to several CiscoWorks applications on one window (including Show Commands and Real-Time Graphs) to monitor router activity.
- Contacts—Provides quick access to find the emergency contact person for a particular device.
- Log Manager—Enables you to store, query, and delete messages gathered from CiscoWorks applications and Cisco Systems devices on the internetwork.

These applications enhance your capabilities as a network administrator to set up diagnostic procedures when your network develops problems. The applications are discussed in detail in the following sections.

Certain applications in CiscoWorks Release 1.0(2) and later have been enhanced by the addition of a retry popup window. This popup window indicates the loss of connectivity to a device and enables you to retry the request or quit. The popup window displays the following message:

```
Device router-name not responding to SNMP
```

The retry popup window appears in the following CiscoWorks applications:

- Path Tool—Skips a hop and proceeds normally until it completes its task. Path Tool reports devices that did not respond to SNMP.
- Environmental Monitor—Restarts the timer and proceeds when the Cisco device is available.
- Show Commands—No timer is available, but the Show Commands application continues when the Cisco device is available.
- Health Monitor—Restarts the timer and proceeds when the Cisco device is available.

Figure 3-1 illustrates how to access CiscoWorks applications from the SNM Tools menu. Figure 3-2 illustrates how to access CiscoWorks applications from the SNM Glyph menu. The grayed-out tools are SNM tools.

Figure 3-1 CiscoWorks Applications on the SNM Tools Menu

Figure 3-2 CiscoWorks Applications on the SNM Glyph Menu

Troubleshooting Scenarios

You can use CiscoWorks applications to troubleshoot your network faults. Table 3-1 describes network problems and recommends CiscoWorks applications to help you troubleshoot and repair the problem. To use the table, locate the problem description that most closely resembles your current situation. Then perform the recommended tasks until you uncover the solution to the problem.

Note: Perform the tasks in Table 3-1 before you contact your technical support person. Make sure you are ready to supply the information found in the "Service and Support" section in the front of this manual.

Table 3-1 Troubleshooting Scenario Tables

Problem	CiscoWorks Application Recommendation
Suspected problem on a network device	Use Device Manager to find the vendor to contact for assistance. Refer to “Vendors Window” in the “Device Management” chapter.
	Use Device Manager to get specific data on a device (serial number, software version, and so on). Refer to “Devices Window” in the “Device Management” chapter.
	Use Device Monitor to monitor environment and interface statistics. Refer to “Monitoring Network Devices” later in this chapter.
	Use Path Tool to check the graphical path for link utilization analysis. Refer to “Locating Device Routing Paths” later in this chapter.
	Use Environment Monitor to check the voltage and temperature of Cisco routers. Refer to “Monitoring Your Device Environment Statistics” later in this chapter.
	Use Show Commands to get data on the version, interface, and so on for analysis. Refer to “Using Show Commands to View Router Data” later in this chapter.
	Use Configuration Management to compare present and previous configurations for errors. Refer to “Comparing Configuration Files” in the “Managing Cisco Device Configurations” chapter.
	Use Contacts data to get information on who to call in your company. Refer to “Using Device Contacts” later in this chapter.
	Check the Log Manager file for event information. Refer to “Using Device Contacts” later in this chapter.
Suspected protocol problem	Check Log Manager for event information. Refer to “Using Device Contacts” later in this chapter.
	Check Device Monitor to ensure you are monitoring events (and interfaces). Refer to “Monitoring Network Devices” later in this chapter.
	Use Path Tool to determine if the protocol is routing efficiently (link speed, utilization and error analysis). Refer to “Locating Device Routing Paths” later in this chapter.
	Use Show Commands to determine packet information using show traffic mix. Refer to “Using Show Commands to View Router Data” later in this chapter.
	Use Real-Time Graphs to get information on router traffic. Refer to “Graphing Your Real-Time Device Data” later in this chapter.

Problem	CiscoWorks Application Recommendation
Router configuration problems	Do a **Show Version** to ensure version numbers are compatible. Router software must be Software Release 8.2 or later. Refer to "Using Show Commands to View Router Data" later in this chapter. Log onto the device and check if the device configuration file has a read-write community string. Refer to "Comparing Configuration Files" in the "Managing Cisco Device Configurations" chapter. Also see this table's recommendation under the "Suspected problem on a network device" entry. Verify the device is running (show interface, show traffic mix). Refer to "Using Show Commands to View Router Data" later in this chapter. Check if a configuration file was downloaded to a device with syntax errors in it. (Log on to router console and initiate a TFTP session from the router. The errors will be displayed on your console screen.) Or log on to the router before you download a file. Check to see if any error messages exist. Refer to "Loading a Configuration File" in the "Managing Cisco Device Configurations" chapter.

Monitoring Network Devices

CiscoWorks provides the Device Monitor (nmdevmon) application to monitor interface and environmental card status and to filter event messages. It also provides a summary of the current devices and the categories that are being monitored.

The Device Monitor also enables you to set how often to poll each device for interface and environment information, or to enable event logging. Because the Device Monitor polls each device according to a set polling frequency, this can add significantly to your network traffic. The default polling frequency rate is 60 seconds. The recommended minimum polling interval depends on the number of devices you are polling and how much network bandwidth you want to devote to network management.

Note: The Device Monitor does not provide text or graph reports, but enables CiscoWorks to monitor devices and filter event messages for those devices to the Log Manager and SNM Console. For log message data, refer to "Using the Log Manager as a Diagnostic Tool" later in this chapter. For environmental monitor data, refer to "Monitoring Your Device Environment Statistics" later in this chapter. For data collected on interfaces, refer to any of the CiscoWorks applications that provide interface data, including Show Commands, Health Monitor, and Device Polling.

The Device Monitor uses a monitoring engine called the Device Monitor daemon (nmdevmond) to perform the following functions:

- Poll for environment and interface statistics.
- If SNM is running, the Device Monitor places an event in the SNM Console log file which forwards it to the CiscoWorks Log Manager via the Event Logger daemon (nmeventd). The Event Logger daemon reads SNM event and trap reports and forwards these messages to the Log Manager. SNM uses this data to change the glyph state (up or down) for status updates. If the SNM Console is not running, the Device Monitor daemon places an event message in the Log Manager.

Set monitoring requirements in the Device Monitor window; the Device Monitor daemon uses these requirements to perform its monitoring tasks.

Note: If a device only has a single interface and that interface fails, the Device Monitor daemon will not send an event to the SNM Console. This is because the Device Monitor daemon realizes that the device is inaccessible and cannot check the interface status. To check device status, you can configure your SNM automatic node management. Refer to "Configuring SNM Console Properties" in the "Using CiscoWorks on SNM" chapter or to your *SunNet Manager 2.0 Reference Guide*. In order to avoid redundant polling and the sending of event messages to the SNM Console and Log Manager, CiscoWorks does not poll for this type of status events.

Figure 3-3 illustrates the process that CiscoWorks uses when monitoring devices.

Note: If you check the environment monitoring option and the device you are polling does not have the proper environmental card, the Log Manager will contain an error message.

Figure 3-3 Device Monitoring Process

Device Monitor Primary Window

Figure 3-4 illustrates the Device Monitor window. Table 3-2 describes the components in this window.

Figure 3-4 Device Monitor Window

Table 3-2 Device Monitor Window Components

Component	Subcomponent	Description
File	Print	Prints a snapshot of the current window.
	Version	Displays the CiscoWorks version information for this application.
	Quit	Exits the current window.
Options	Activate Changes	Updates polling to new values.
	Set Polling Frequency	Changes the polling rate. The default is 60 seconds.
	Summary	Provides an overview of which monitoring options are on or off and what interval is set for polling.

Component	Subcomponent	Description
Security	Privileges	Displays the current user's security privileges.
	Change User	Enables you to change your username in order to access this application.
Help		Provides help text on the current window.
Select All		Selects all devices in the device browser.
Deselect All		Deselects all devices in the device browser.
Polling Frequency	Polling Interval Slider	Changes the polling rate by clicking on the slider. The default is 60 seconds.
Check Boxes	Log Events	Filters log messages sent to the event logging daemon.
	Monitor Environment	Monitors environmental monitor card data on the Cisco AGS+ router.
	Monitor Interfaces	Monitors interface status information.
Apply		Applies changes to selected devices to the Sybase devices table.

Setting Device Monitoring Options

To set device-monitoring options, perform the following steps:

Step 1: From the main SNM Tools menu, pull down to **Device Monitor**.

The Device Monitor window appears. See Figure 3-4.

Step 2: Select the devices you want to change. To set individual device monitoring options, click on the device or devices in the scroll window. To set all devices at once, click on **Select All**.

Step 3: Change the default polling frequency by using the Polling Interval Slider or type over the default in the polling interval field and press Return.

You can also use the Option menu to set the polling frequency. If you do so, the Polling Frequency window appears. Enter your new polling rate and click on **OK**. See Figure 3-5.

Figure 3-5 Polling Frequency Window

Step 4: Select the categories of options (environment, interfaces, and/or events) by clicking on the check boxes next to the desired option.

Step 5: Accept monitoring designations by clicking the **Apply** button.

Step 6: Select **Activate Changes** from the Options menu to send the changes to the device monitoring daemon.

After your changes are sent to the device monitoring daemon, the Device Monitor begins polling your designated options.

Time Saver: To set all device-monitoring options at once, click the **Select All** button. Then choose your options (environment, events, and/or interfaces) and your polling frequency, if necessary. Click the **Apply** button. To deselect all your devices monitoring options, click the **Deselect All** button then click on the **Apply** button.

To exit the Device Monitor window, pull down the File menu and select **Quit**.

Adding Devices to the Database from SNM

The Device Monitor can only monitor devices that exist in the Sybase device table. If a new device has been added to SNM manually or via the SNM Discover program, the Device Monitor will not see it until you perform one of the following tasks:

- Add the device manually to the Sybase device table using the device form in the Device Management application.

  Refer to “Building Devices Data” in the “Device Management” chapter for information on how to enter device information.

- Run Sync w/Sybase to synchronize devices from Sun’s database to the CiscoWorks Sybase database. You can use either the Glyph or Tools menu to access Sync w/Sybase.

  Refer to the “Device Management” chapter for information on how to use Sync w/Sybase.

Viewing Device Monitor Settings in the Summary Window

You can quickly view the following device monitor settings with the Device Monitor Summary window:

- Frequency
- Events data
- Environmental data
- Interface data

Figure 3-6 illustrates the Summary window for the Device Monitor. Table 3-3 describes the components in this window.

Figure 3-6 Summary Window for the Device Monitor

Table 3-3 Summary Window Components

Component	Subcomponent	Description
File	Print	Prints a snapshot of the current window.
	Version	Displays the CiscoWorks version information for this application.
	Quit	Exits the current window.
Help		Provides help text on the current window.
Device list		List of network devices known to Sybase.
Polling Frequency		Current polling rate on this device.
Events data		Indicates whether monitoring is on (y) or off (n).
Environmental data		Indicates whether monitoring is on (y) or off (n).
Interface data		Indicates whether monitoring is on (y) or off (n).
Search String field		Provides field for character string to locate in text.

Component	Subcomponent	Description
Search Forward		Searches forward for a character or character string in the text.
Search Backward		Searches backward for a character or character string in the text.

To view your device monitor settings, perform the following steps:

Step 1: From the Device Monitor window, select Option and pull down to **Summary**.

The Device Monitor Summary window appears.

Step 2: Search for a specific device by entering the device name in the Search String field.

Step 3: Click on **Search Forward** or **Search Backward**.

To exit the Device Monitor Summary window, select the File menu and pull down to **Quit**.

Monitoring Your Device Environment Statistics

With Software Release 9.0, Cisco has enhanced the environmental monitor card on the AGS+ router. Specifically, several features were added to allow the monitoring of temperature and voltage sensors via SNMP. Your environmental monitor card must be a Rev. 4 ENVM card (Microcode Version 2.0) or later.

The CiscoWorks Environmental Monitor application enables you to view a device's environmental monitor status including temperature and voltage statistics. The default temperature displayed is in Celsius.

Note: Each device has a default polling frequency rate of 60 seconds. This rate was chosen because the environmental monitor card only updates its information internally every 60 seconds. This feature is not meant to replace your router console's critical log information, but to provide you with a graphical view of the environmental monitor card with the click of a button.

If you want environmental monitor card version or hardware information, use the **Show Commands** application under the SNM Glyph Tools menu.

Refer to the configuration note, "Installing and Configuring the Environmental Monitor Card in the AGS+ Chassis," for more information on the environmental monitor card features.

Environmental Monitor Window

Figure 3-7 illustrates the Environmental Monitor window. Table 3-4 describes the components in this window.

Figure 3-7 Environmental Monitor Window

Table 3-4 Environmental Monitor Window Components

Component	Subcomponent	Description
File	Print	Prints a snapshot of the window.
	Version	Displays the CiscoWorks version information for this application.
	Quit	Exits the current window.
Options	Change To Celsius	Toggles temperature setting to Celsius.
	Change To Fahrenheit	Toggles temperature setting to Fahrenheit.
Help		Provides help text on the current window.
Date stamp		Provides the date and time the window was created.
Polling Frequency	Polling Interval Slider	Changes the polling rate by clicking on the slider. The default is 60 seconds.

Component	Subcomponent	Description
Voltage meters	+5 voltage	Current power supply voltage to the router.
	-5 voltage	Current power supply voltage to the router.
	+12 voltage	Current power supply voltage to the router.
	-12 voltage	Current power supply voltage to the router.
Temperature meters	Internal temperature	Current internal intake air temperature for the router.
	Airflow temperature	Current exhaust air flow for the router.

Monitoring Your Router Environmental Data

To use the Environmental Monitor to check a device's temperature and voltage, perform the following steps:

Step 1: Click on the device and pull down to the Tools submenu.

Step 2: Pull over to the **Env. Monitor** command.

The Environmental Monitor window appears.

Step 3: To change from Celsius to Fahrenheit, pull down the Option menu and select **Change to Fahrenheit**.

The window automatically updates and reappears with Fahrenheit temperatures.

Step 4: To change the polling frequency, use the polling interval slider or type over the default in the polling interval field.

Step 5: To print the screen, pull down the File menu to **Print**.

The Sun Snapshot window appears. For more information on how to use the Snapshot utility, refer to the SunOS manual.

Locating Device Routing Paths

The Path Tool application graphically displays the routing path between a source device and a destination device using the standard protocols (SNMP or IP). The Path Tool application illustrates a path between a source and a destination device and displays that path in the Path Tool window. This application enables you to check the paths between two IP addresses.

The graphical display in the Path Tool window shows the devices (including routers) involved, the link speeds connecting these SNMP devices, and the interface names. You can run several Path Tool analyses at the same time. Each Path Tool request appears in a separate window.

Note: If a device is not accessible using SNMP, the analysis confirms this and uses other methods to discover the path. However, for best results, network devices should have SNMP turned on.

You can access the Path Tool application from the Tools menu for all devices, or from the Glyph menu to access a specific device as the source device.

You need to work with several windows to use the Path Tool application:

- Path Tool source and destination form—You enter source and destination data. See Figure 3-9.
- Path Tool route path window—All devices from the source to the destination device display with device name, IP address, link speed, interface names, and color-coded threshold information. See Figure 3-8.
- Path Tool path hops text window—The Path Tool displays the path hop information from the source device to the destination device. See Figure 3-11.

  This is the main Path Tool window that you need to understand. This same window is used during the utilization and error analysis. It is described in detail in the following section.
- Path Tool Properties window—You set utilization and error severity thresholds to mark interfaces with appropriate colors. See Figure 3-14.

Path Tool Window

Figure 3-8 illustrates the Path Tool route path window, which is the primary Path Tool window. Table 3-5 describes the components in this window.

Figure 3-8 Path Tool Route Path Window

Note: A black link in a path displayed in the Path Tool window indicates that the device did not respond to SNMP.

Table 3-5 Path Tool Window Components

Component	Subcomponent	Description
File	Print	Prints a snapshot of the current window.
	Version	Displays the CiscoWorks version information for this application.
	Quit	Exits the current window.
Analysis	Utilization	Performs an analysis on link utilization.
	Errors	Performs an analysis on errors per second.
View	Utilization	Toggles to the path showing utilization analysis.
	Errors	Toggles to the path showing error analysis.
Options	Properties	Displays analysis settings, polling interval, and severity levels.
	Re-discover Path	Displays alternative routing path, if found.
Help		Provides help text on the current window.
Interface Names		Displays the first letter of the interface type and the interface number. The abbreviation is the first character of the interface description attached to the interface number. The following list includes the interface-type abbreviations for Cisco interfaces: ■ E=Ethernet ■ F=FDDI ■ S=Serial ■ T=Token Ring ■ U=Unknown via SNMP
Link Speeds		Displays the link speed between interfaces in Mbps or Kbps (megabits or kilobits per second). If an interface is unknown, the link speed is represented by three question marks (???).

Using Path Tool from the SNM Tools Menu

If you cannot find your source device icon on the network map or you do not know the device information, use the SNM Tools menu to access the **Path Tool** application. The following procedure enables you to choose your source or destination device from a list of device names.

To display an analysis of the entire path or any valid subpath using the SNM Tools menu, perform the following steps:

Step 1: From the Tools menu, pull down to **Path Tool**.

The Path Tool Source/Destination window appears. See Figure 3-9.

Figure 3-9 Path Tool Window—Source/Destination Window

Step 2: Enter the source device name.

The path source is the device you want the path to start from. If you do not know the source device name, press the **Select** button. A Device Selection window appears. See Figure 3-10.

Select your source device from the scroll window and press **OK**.

Figure 3-10 Device Selection Window

Step 3: Enter a path destination.

The path destination is the device you want the path to end with. If you do not know the destination device name, press the **Select** button. A device selection window appears.

Choose a device and press **OK** to close the Device Selection window.

Step 4: Press **OK** in the Path Tool window.

The Path Tool uses a text browser to display the path hops from the source device to the destination device. See Figure 3-11.

Figure 3-11 Path Tool Window—Path Hops from Source to Destination

After the Path Tool reaches the destination, it displays a picture of the route. This is the known path from your source device to your destination device. Use the scroller at the bottom of the window to view the full path route if it is too large to fit into the window. See Figure 3-8.

In Figure 3-8, the source device is a UNIX workstation with a host name of *smith-ws*. An interface named le0 connects the source device to the AGS+ router, *abc.cisco.com*, at a link speed of 10 Mbps. The host name *su-b.abc.com*, with an FDDI interface *F0*, connects to a Token Ring. The Token Ring connects to host address 192.31.48.244 at a link speed of 100 Mbps. Note that the interfaces on this host address are marked with a U (unknown). This indicates that the SNMP protocol was not used to find the route through this device.

Using Path Tool from the Glyph Menu

You can also run the Path Tool application from the Glyph menu. The Glyph menu is SNM's pull-down menu for a particular device. This procedure enables you to choose your destination device from a list of device names. The source device information is automatically entered after you click on the Cisco icon representing your source device.

To display an analysis of the entire path or any valid subpath using the Glyph menu, perform the following steps:

Step 1: From the SNM Console window, click on a device.

This is the source device you want the path to start from.

Step 2: Select the Glyph menu by placing your pointer on the desired device and selecting **Path Tool** from the Tools submenu. See Figure 3-12.

Figure 3-12 Glyph Menu with Tools Submenu Applications

The Path Tool window appears. Note that the source device is automatically entered in the window. See Figure 3-13.

Figure 3-13 Glyph Path Tool Source/Destination Window

Step 3: Enter a path destination.

The path destination is the device with which you want the path to end. If you do not know the destination device name, press the **Select** button. A device selection window appears.

Choose a device and press **OK** to close this window.

Step 4: Press **OK** in the Path Tool window.

The Path Tool window appears.

Step 5: Refer to the previous section, "Using Path Tool from the SNM Tools Menu," for the results of the Path Tool process.

Path Tool Properties Window

The Properties window is the key to setting your analysis parameters. You can set continuous utilization and error analyses and your polling interval from the Properties window. You can also set a text window to appear each time a utilization or error analysis is performed. This text window contains statistics displayed in the Path Tool window.

After you run the Path Tool application, you can access the Properties window from the Options menu. Figure 3-14 illustrates the Path Tool properties window. Table 3-6 describes the components in this window.

Before you perform an analysis, you might want to access the Properties window to set your parameters. You can choose to use the CiscoWorks defaults to run the Path Tool application.

Figure 3-14 Path Tool Properties Window

Table 3-6 Path Tool Properties Window Components

Component	Subcomponent	Description
Utilization	Show Text	If activated, Show Text displays a window with utilization analysis data.
	Continuous	If activated, a Path Tool window runs continuously, rediscovering a specific path's utilization data using the set polling interval.
Errors	Show Text	If activated, Show Text displays a browser window with error analysis data.
	Continuous	If activated, a Path Tool window runs continuously, rediscovering a specific path's error data using the set polling interval.
Polling Frequency	Polling Interval Slider	Changes the polling rate by clicking on the slider. The default is 15 seconds.
Utilization Severities	Level 1 to 5	Threshold settings for utilization color codes in percent. Thresholds must be in ascending order.
Error Severities	Level 1 to 5	Threshold settings for error color codes in errors per second. Thresholds must be in ascending order.

Setting Parameters in the Path Tool Properties Window

To change the settings in the Path Tool Properties window, use the following steps:

Step 1: On the Path Tool window, select the Options menu and pull down to **Properties**.

Step 2: Change any of the following settings:

- To activate a text browser window that displays a report of the utilization or error analysis Path Tool window, click on the appropriate **Show Text** check box.

  The next time you run an analysis, a text window will display immediately before the Path Tool window updates. Use **Show Text** to troubleshoot a network problem.

- To activate a continuous utilization or error analysis (which runs using the polling interval), click on the appropriate **Continuous** check box.

  When you run an analysis, CiscoWorks will use the polling interval to rerun the analysis until the Path Tool window is closed. Use **Continuous** to determine the performance of your network, since several path analyses can be compared.

- To change the polling interval for continuously rediscovering this path, click on the polling interval field and enter your new interval over the old interval rate.

  The next time CiscoWorks rediscovers this path, it will use the new polling interval.

- To change the utilization severities, click on the field of the level you want to change and enter the severity level threshold (in percents).

  The next time the path is rediscovered or a new path is tracked, the new thresholds are used to color code the links.

- To change the error severities, click on the field of the level you want to change and enter the severity level threshold. (in errors per second)

  The next time the path is rediscovered or a new path is tracked, the new thresholds are used to color code the links.

Step 3: When you have changed your property settings, click on **OK** to save your property parameters.

Note: You cannot change the color codes in the Properties window. If you change severity levels, keep them in ascending order.

Analyzing a Graphical Path

The Path Tool enables you to run two types of analysis to measure network activity. This analysis can only be performed on devices with SNMP access. The two types of analysis include:

- Utilization analysis—Measures the average percent of bandwidth used by all traffic on an interface in real time.
- Error analysis—Measures the packets with errors as a percentage of total packets (good packets plus error packets) on an interface or on all interfaces on the path.

Refer to the previous section, "Setting Parameters in the Path Tool Properties Window," for more information on changing the defaults in your Properties window. A description of the types of analysis follows.

Utilization Analysis

The utilization analysis function does two things: color codes the links in the path window and provides an optional browser window that shows the usage of each link when you select Show Text on the Properties window.

Each link between devices is assigned a color based on settings in the Properties window. You can change these utilization settings depending on your network needs.

The Path Tool provides the following defaults for the utilization settings:

- Green: Level 1–0%
- Blue: Level 2–5%
- Yellow: Level 3–10%
- Orange: Level 4–15%
- Red: Level 5–20%

Note: A black link in a path displayed in the Path Tool window indicates that the device did not respond to SNMP.

For example, in the Path Tool utilization window, a green link means that the link is using between 0 and 5 percent of the bandwidth. Figure 3-15 shows the Path Tool with the color-coded links. The defaults describe how the color codes relate to real utilizations. For example, green might signify less than 10 percent use, while red might mean over 90 percent utilized. You can set the utilization and error severities in the legend on the Properties window.

Figure 3-16 shows a color plate of the Properties window that the Path Tool uses to determine what colors to assign to the link status of each line. A key to parameter settings is found on the Properties window.

Utilization analysis also provides a browser window showing the actual usage for each link in numerical order. This analysis can be found using the View menu on Path Tool. The utilization analysis measures both ends of the link.

Error Analysis

The error analysis function is similar to utilization analysis. However, instead of color coding the real utilization analysis, the Path Tool color codes the errors per second on the link. Each link between devices is assigned a color based on settings in the Properties window. You can change these error settings based on your network needs.

The Path Tool provides the following defaults for the error analysis settings:

- Green: Level 1–0 errors/second
- Blue: Level 2–5 errors/second
- Yellow: Level 3–10 errors/second
- Orange: Level 4–15 errors/second
- Red: Level 5–20 errors/second

Note: A black link in a path displayed in the Path Tool window indicates that the device did not respond to SNMP.

For example, in the Path Tool error utilization window in Figure 3-19, if a link is blue this link is seeing from five to ten errors per second. The interface error measurement includes packets with errors as a percentage of total packets (good packets plus error packets) on an interface.

Figure 3-16 shows the Properties window that the Path Tool uses to determine what colors to assign to the error status of each line.

As another example, a link with no errors may appear green, while a link with an 80 percent error rate may appear red. The Path Tool only checks errors appropriate to the type of media for the link. For example, on an Ethernet it would look at errors specific to Ethernet interfaces.

Figure 3-15 Path Tool Window with Color-Coded Links

Figure 3-16 Color-Coded Path Tool Properties Window

Running a Utilization Analysis

From the Path Tool window, you can perform a utilization analysis of the data in the window.

To analyze the average percent of bandwidth used by all traffic used in real time, perform the following steps:

Step 1: From the Path Tool window, pull down the View menu and choose Utilization (if you have not already done so).

This toggles to the Path Tool Utilization Analysis window.

Step 2: From the Path Tool window, pull down the Analysis menu to **Utilization**.

The Path Tool window reappears and is timestamped with the utilization analysis confirmation. See Figure 3-17.

Figure 3-17 Path Tool Window After Utilization Analysis

Note: If the Sun workstation generic icon appears in the path route as a device that you know is a Cisco device, perform a **Change Type** command or create a component and choose a Cisco-specific or appropriate device icon to represent the device on the map.

A Utilization text window also appears if you chose **Show Text** on the Properties window. See Figure 3-18.

Figure 3-18 Utilization Analysis Text Window

The Utilization text window contains data on the percentage of bandwidth each device interface is using in real time.

For example, the Ethernet 0 interface on cisco.barrnet.net is using only 0.1 percent of the bandwidth, while the Ethernet 1 interface at su-a.STANFORD.EDU is utilizing 8.1 percent of the bandwidth. Each network administrator must determine what utilization percentage is within the acceptable ranges. Note that for device 192.31.48.244, which does not have SNMP enabled, shows a percentage as U (unknown).

Step 3: If you have a large scale path, you can search forward or backward for any character string. For example, you might want to search for a device name, an interface name, or a certain percentage. Move your cursor into the window and enter the word **Ethernet2** and click on **Search Forward**. If an Ethernet 2 interface is present in this path, the Utilization text window finds it and highlights it within the browser.

Step 4: Print the Utilization text window's data to a line printer by selecting the File menu and pulling down to **Print**.

Step 5: Save the Utilization text window's data to a file by selecting the File menu and pulling down to **Save**.

Step 6: Exit the Utilization text window and return to the Path Tool window by selecting the File menu and pulling down to **Quit**.

Running an Error Analysis

From the Path Tool window, you can perform an error analysis on the data in the window.

An error analysis collects different information depending on what type of interface your device has. Table 3-7 describes the error analysis variables for non-Cisco and Cisco devices according to their interface types.

Table 3-7 Error Analysis Variables

Interface	Objects Polled	MIB Objects Names
Non-Cisco device (all interfaces)	Input errors Output errors	*ifInErrors* *ifOutErrors*
Cisco device—Ethernet	Collisions Runts Giants CRCs Restarts Resets	*locIfInCollisions* *locIfInRunts* *locIfInGiants* *locIfInCRC* *locIfRestarts* *locIfResets*
Cisco device—serial	Frame errors Overruns Ignoreds Aborts Restarts Resets Carrier transitions	*locIfInFrame* *locIfInOverrun* *locIfInIgnored* *locIfInAbort* *locIfRestarts* *locIfResets* *locIfCar Trans*
Cisco device—FDDI or Token Ring	Runts Giants CRCs Restarts Resets	*locIfInRunts* *locIfInGiants* *locIfInCRC* *locIfRestarts* *locIfResets*

Note: For consistency, this manual uses the term object as a replacement for such terms as MIB variables, MIB object instances, and so on. Other Cisco manuals may use different terms, but they can be used interchangeably.

To analyze the number of packets with errors as a percentage of total packets (good packets plus error packets) in real time, perform the following steps:

Step 1: From the Path Tool window, pull down the View menu and select Errors.

This toggles to the Path Tool Errors Analysis window.

Step 2: From the Path Tool window, pull down the Analysis menu to **Errors**.

The Path Tool window reappears timestamped with the error analysis confirmation. See Figure 3-19.

Figure 3-19 Path Tool Window After Error Analysis

An Errors text window also appears if you chose **Show Text** in the Properties window. See Figure 3-20.

Figure 3-20 Errors Text Window

The Errors window contains data on the percentage of errors per second based on the type of line (Ethernet, serial, Token Ring, FDDI).

For example, in Figure 3-20, smith-ws is a Sun workstation. Since this device is not a Cisco device, only statistics on input and output errors are collected. The Cisco device, abc.CISCO.COM, has an Ethernet connection, so statistics are gathered for collisions, runts, giants, CRCs, restarts, and resets. The serial connection on abc.CISCO.COM gathers statistics on frame errors, overruns, ignoreds, aborts, restarts, resets, and carrier transitions.

Step 3: If you have a large scale path, you can search forward or backward for any character string. For example, you might want to search for a device name, an interface name, or a certain percentage. Move your cursor into the window, enter the word **carrier transitions**, and click on **Search Forward**. If a serial line is present in this path, the Errors text window will find it and highlight it within the browser.

Step 4: Print the Errors text window data to a line printer by selecting the File menu and pulling down to **Print**.

Step 5: Save the Errors text window's data to a file by selecting the File menu and pulling down to **Save**.

Step 6: Exit the Errors text window and return to the Path Tool window by selecting the File menu and pulling down to **Quit**.

Note: If the Path Tool is using methods other than SNMP to discover a path, it may encounter difficulties determining the correct path where parallel routers with parallel links exist. Such a setup appears in Figure 3-21. The way to avoid this problem is to enable SNMP on one of the two parallel devices.

Figure 3-21 Parallel Routers with Parallel Links

Graphing Your Real-Time Device Data

The Real-Time Graphs application monitors the behavior of devices suspected of operating in a degraded mode or introducing erratic behavior in traffic patterns, error status indications, or statistics. Use the Errors and the Queues interface health buttons for quick information about diagnosing problems in your network. Errors and Queues are the only buttons on the Real-Time Graphs window explained in this chapter.

Real-Time Graphs is also useful for managing and planning network loads and use. Refer to “Using the Real-Time Graphs” in the “Performance Management” chapter for more information on performance management.

The Real-Time Graphs application monitors and graphs variables for a single device. Multiple devices can be monitored simultaneously by opening more than one application. In addition, you can merge graphs to present the data in one graph.

Since the Real-Time Graphs application uses the SNM Grapher, information on customizing your graph can be found in the *SunNet Manager 2.0 User’s Guide*.

Real-Time Graphs Window

Figure 3-22 illustrates the Real-Time Graphs window. Table 3-8 describes the components in this window.

Figure 3-22 Real-Time Graphs Window

Note: In Figure 3-22, the device named *pag.cisco.com* does not have the following protocols activated: DECnet IV, Novell, VINES, and XNS. Grayed-out buttons on CiscoWorks application windows indicate inactive functions.

Table 3-8 Real-Time Graphs Window Components

Component	Subcomponent	Description
File	Print	Prints a snapshot of the window.
	Version	Displays the CiscoWorks version information for this application.
	Quit	Exits the current window.
Options	Set Polling Frequency	Changes polling rate. Can be set using slider or typing in on the polling interval field and pressing Return. Default = 2 seconds.
Help		Provides help text on the current window.
Router Health	Buffer Space CPU Load Environment Free Memory Security	Refer to Table 4-5 in the "Performance Management" chapter for a detailed description of the router health buttons.
Interface Health	Bits/Sec Bytes Errors Packets/Sec Packets Queues	Refer to Table 4-6 in the "Performance Management" chapter for a detailed description of the interface health buttons.
Protocol Traffic[1]	IP ICMP SNMP TCP UDP AppleTalk DECnet IV Novell VINES XNS	Refer to Table 4-7 in the "Performance Management" chapter for a detailed description of the protocol traffic buttons.

[1]If a button is grayed out, the selected device does not have this capability. For example, currently only a Cisco AGS+ router with the correct environmental monitor card (Rev. 4) has the Environment router health button capability.

Creating a Real-Time Graph for Interface Error Data

To create a graph with real-time device data (specifically for error information), perform the following steps:

Step 1: Click on a Cisco device and pull down to the Tools menu.

Step 2: Pull over to **Real-Time Graphs**.

The Real-Time Graphs window appears. See Figure 3-23.

Figure 3-23 Real-Time Graphs Window

Step 3: Gather data on interface health by clicking on either the **Errors** or **Queues** button. For this example, click on **Errors**.

These buttons collect MIB object information that will assist you in diagnosing your network problem. Table 3-9 describes these buttons and MIB object descriptions they poll.

Note: CiscoWorks polls differently for Cisco and non-Cisco devices. See Table 3-9 for a list of MIB objects polled by Interface Health buttons.

Table 3-9 Interface Health Buttons—Errors and Queues

Buttons	Description	MIB Object Descriptions
Errors	Displays the number of input packets with various characteristics for *Cisco-specific* devices.	For Ethernet, 802.3 CSMA/CD, starLAN: *locIfCollisions* *locIfInRunts* *locIfInGiants* *locIfInCRC* *locIfResets* *locIfRestarts* For FDDI and Token Ring: *locIfInRunts* *locIfInGiants* *locIfInCRC* *locIfResets* *locIfRestarts* For serial (Cisco-specific): *locIfInFrame* *locIfInOverrun* *locIfInIgnored* *locIfInAbort* *locIfResets* *locIfRestarts* *locIfCarTrans*
	Displays the number of input packets with various characteristics for any *non-Cisco* devices.	For serial (non-Cisco): *ifInErrors* *ifOutErrors*
Queues	Displays the number of packets dropped because the input or output queue was full for *Cisco-specific* devices.	*locIfInputQueueDrops* *locIfOutputQueueDrops*

The real-time graphs you create use the polling frequency that appears in the window. You can enter a new polling frequency.

Step 4: After you click on the **Errors** button, a grapher window appears.

Figure 3-24 displays the real-time graph for errors.

Seconds later, a Results Grapher window also appears. The devices and variables you selected appear in the scroller window.

Figure 3-24 Graph Window for Errors Statistics

Caution: When you are finished, you must remove graphs using the Results Grapher window or they will continue to poll.

Viewing or Changing Graph Properties

The Real-Time Graphs application uses SNM's Grapher. If you want to change the appearance of your real-time graph, you need to use SNM's Results Grapher window. See Figure 3-25.

Figure 3-25 SNM Results Grapher Window

You can perform the following tasks using the Results Grapher:

- View different graphs listed in the Results Grapher browser.
- Access a properties pop-up window to change graph properties such as color, plot values, and scaling parameters.
- Remove or halt real-time graphs data collection.
- Merge two or more graphs.

Note: Refer to the *SunNet Manager 2.0 User's Guide* for more information on the SNM Grapher.

Using Show Commands to View Router Data

CiscoWorks provides a unique interface to Cisco routers or communication servers on your network. Using the **Show Commands** application, you can view device data with the click of a mouse.

Show Commands Window

Figure 3-26 illustrates the Show Commands window. Table 3-10 describes the components in this window.

Figure 3-26 Show Commands Window

Note: The inactive (grayed-out) **Show Environment** button in Figure 3-26 means the selected device does not recognize the Rev.4 environmental monitor card. You might not have the correct card or the device might not support retrieval of information via SNMP.

Table 3-10 Show Commands Window Components

Component	Definition	When to Use
File Print Version Quit	 Print a snapshot of the window. Display CiscoWorks version information for this application. Exit the current window.	To perform the tasks described in the previous column.
Help	Provides help text for the current window.	
Show Buffers	Displays statistics for the buffer pools on the network server.	If the input queue count on an interface is consistently nonzero. Use to determine if you need to adjust initial buffer pool settings and the limits at which temporary buffers are created and destroyed
Show Environment	Displays temperature and voltage information.	If you have received a warning or shutdown message; query the environmental monitor card to determine if a measurement is at a warning tolerance. Available only on devices with environmental monitor cards, for example, the Cisco AGS+ router.
Show Flash	Displays information about the Flash memory on a Cisco device.	If you want to check the amount of Flash memory available or the file(s) stored in Flash.
Show Interface	Displays status of device interfaces.	If you have a problem after reconfiguring a device. You can also use it as a monitoring tool.
Show Traffic Mix[1]	Displays status information on all protocol traffic.The window contains device, protocol, and interface data.	If you want to check protocol traffic activity.
Show Version	Displays the selected device's software title and version and cumulative uptime since last reload of the software. For routers running Software Release 9.1, this window displays traffic per protocol on each interface.	If it is necessary to contact technical support; have all version information ready for your technical support specialist.
Show IP Accounting Checkpoint	Displays the checkpointed accounting database, which contains source and destination addresses and the total number of packets and bytes for each address pair.	If you want to check accounting database information.

Component	Definition	When to Use
Show IP ARP	Displays the Address Resolution Protocol (ARP) cache.	If you want to check the records of each network address's correspondence (an IP address, for example) and LAN hardware addresses (MAC addresses).
Show IP Route	Displays the current state of the IP routing table.	If you want to check routing information.
Show AppleTalk Traffic	Displays AppleTalk traffic statistics.	If you want to check information on AppleTalk-specific traffic.
Show DECnet Traffic	Displays DECnet traffic statistics.	If you want to check information on DECnet-specific traffic.
Show IP Traffic	Displays IP statistics.	If you want to check IP traffic information.
Show Novell Traffic	Displays Novell traffic statistics.	If you want to check Novell-specific traffic information.
Show VINES Traffic	Displays VINES traffic statistics.	If you want to check VINES-specific traffic information.
Show XNS Traffic	Displays XNS packet statistics.	If you want to check XNS-specific traffic information.

[1]**Show Traffic Mix** is a feature specific to CiscoWorks, and is not a router EXEC **show** command.

Note: Show Commands information provided using the CiscoWorks software differs slightly from the **show** commands performed directly at the router console. The difference in statistics may occur if information is not available through the SNMP protocol.

Accessing the Show Commands Windows

To access the individual Show Commands windows, perform the following steps:

Step 1: Click on a Cisco network device and pull down to the Tools submenu.

Step 2: Pull over to the **Show Commands** command.

The Show Commands window appears.

Step 3: To request specific system status, IP information, or traffic information, click on the desired Show Commands button. Several show windows are described below.

Step 4: Exit the Show Commands window by selecting the File menu and pulling down to **Quit**.

For more detailed information on **show** commands, refer to the *Router Products Configuration and Reference* publication.

Show Commands Subwindows

Figure 3-27 illustrates a Show Commands subwindow. Table 3-11 describes the components of the individual Show Commands windows.

The **show** commands listed in Table 3-10 each have their own show window. Because there are several **show** commands, examples of a selection of show windows appear later in this section.

Figure 3-27 Show Commands Subwindow—Show Buffers

Table 3-11 Show Commands Subwindow Components

Component	Subcomponent	Description
File	Print	Prints the contents of the current window.
	Save	Saves the contents of the current window to a file.
	Version	Displays the CiscoWorks version information for this application.
	Quit	Exits the current window.
Option	Refresh	Redisplays the current window with updated data.
Help		Provides a manual page on the current window.
Search String field		Provides a field for the character string to locate in text.

Component	Subcomponent	Description
Search Forward		Searches forward for a character or character string in the text.
Search Backward		Searches backward for a character or character string in the text.

Show Environment Window

From the Show Commands window, click on the **Show Environment** button to display the Show Environment window. See Figure 3-28.

Figure 3-28 Show Environment Window

Note: Your Cisco AGS+ must have the Rev. 4 environmental monitor card (Microcode Version 2.0) in order for the **Show Environment** command to work properly. The network map must also define the device type as an AGS+.

The show environment window displays temperature and voltage information on the AGS+ router console. You can access the Show Environment window to check data after you receive a warning or shutdown message from your AGS+ router.

Show Flash Memory Window

To display information about Flash memory on a Cisco device, click on the **Show Flash** button in the Show Commands window. A Cisco 7000 router would display information similar to the following:

```
4096K bytes of flash memory on embedded flash (in RP1).

file     offset     length        name
  0     0x80        53364       eip1-0
  [4140812/4194304 bytes free]
```

For CiscoWorks Release 1.0(3) caveat information on this feature, refer to the "CiscoWorks Release 1.0(3) Caveats" section in the "Troubleshooting CiscoWorks Errors" appendix.

Show Traffic Mix Window

From the Show Commands window, click on the **Show Traffic Mix** button to display the Show Traffic Mix window. See Figure 3-29.

The Show Traffic Mix window provides all traffic information, regardless of protocol. This command polls the router and shows statistics over a short period of time. Use the **Refresh** button to update this period and recalculate the statistics shown.

This Show Command is a feature specific to CiscoWorks, and is not a router EXEC **show** command. You can use this command as a quick view of traffic activity.

Figure 3-29 Show Traffic Mix Window

The Show Traffic Mix window in Figure 3-29 contains the following three sections:

- Section A—Provides router data on the following information:
  - Router uptime
  - Total packets forwarded
  - Percentage of packets forwarded by each protocol
  - Number of packets forwarded by each protocol

- Section B—Provides router data on the following information:
  - For each interface, the total number of bytes sent and received by the router
  - For each interface, what percentage of the total bytes this represents in the router

- Section C—Provides router data on the following information:
  - For each interface, the total number of packets sent and received by the router
  - For each interface, what percentage of total packets this represents in the router

Show IP Accounting Checkpoint Window

From the Show Commands window, click on the **Show IP Accounting Checkpoint** button to display the Show IP Accounting Checkpoint window. See Figure 3-30.

The Show IP Accounting Checkpoint window displays the checkpointed database. The output contains source and destination addresses, as well as total number of packets and bytes for each address pair. Use this information to check resource usage.

Figure 3-30 Show IP Accounting Checkpoint Window

If there is no IP accounting checkpoint on the selected router, you will receive the error message shown in Figure 3-31.

Figure 3-31 IP Accounting Checkpoint Error Message Popup Window

Show IP Traffic Window

From the Show Commands window, click on the **Show IP Traffic** button to display the Show IP Traffic Window. See Figure 3-32.

The Show IP Traffic window displays statistics on IP protocol operation.

Figure 3-32 Show IP Traffic Window

Querying Device Health

The Health Monitor application provides you with information about the overall health of a device and allows you to access to several CiscoWorks applications on one window.

You can perform the following tasks from the Health Monitor window.

- Access Show Commands buttons for version, interface, buffer, or protocol information.
- Use Real-Time Graphs for interface or protocol information.
- Use Real-Time Graphs for buffer misses, free memory, CPU, interface, or protocol information.

Health Monitor Window

Figure 3-33 illustrates the Health Monitor window. Table 3-12 describes the components in this window.

Figure 3-33 Health Monitor Window

The Health Monitor window in Figure 3-33 contains the following three sections.

- Section A—Provides menu selections and device data on the following information:
  - Device type and name.
  - Buffer misses and free memory data. This data is polled continuously at 15-second intervals by default.
  - CPU load (*busyper*, *avg1*, *avg5*) for current, one-minute and five-minute intervals. This data is polled continuously at 15-second intervals.

- Section B—Provides protocol data on the following information:
  - Percentage of traffic forwarded on this router for a specific protocol.

- Section C—Provides interface data on the following information:
  - Percentage of utilization for this router for a specific interface.

Table 3-12 contains references to two applications. These applications are represented in the window menuing system by the Show Commands and Real-Time Graphs icons. These icons are displayed in Figure 3-34.

Figure 3-34 Health Monitor Window Icons

Table 3-12 Health Monitor Window Components

Component	Subcomponent	Description
File	Print	Prints a snapshot of the window.
	Version	Displays the CiscoWorks version information for the application.
	Quit	Exits the current window.
Options	Properties	Changes polling rate. Default = 60 seconds. Also changes format of free memory from bytes to kilobytes.
Help		Provides help text on the current window.
Device[1]	Show Commands	Provides **Show Version** command.
Buffer Misses	Show Commands	Provides **Show Buffers** command.
	Real-Time Graphs	Provides buffer data graph.
CPU	Real-Time Graphs	Provides CPU data graph.
Free Memory	Real-Time Graphs	Provides free memory data graph.

Component	Subcomponent	Description
Protocols	Show Commands Real-Time Graphs	Provides **show** protocol command. Provides protocol data graph.
Interfaces	Show Commands Real-Time Graphs	Provides **Show Interface** command. Provides interfaces data graph.

[1]An icon representing a device type appears next to the device name in the Health Monitor window. The icon changes depending on the device type. Refer to Chapter 2, "Using CiscoWorks on SNM," for an illustration with all CiscoWorks icons.

Note: All graphs created using the Health Monitor inherit the polling interval setting from the Health Monitor window.

Figure 3-35 illustrates the following Show Commands and Real-Time Graphs applications you can access from within the Health Monitor window:

- Show Version
- Shop IP Traffic
- Free Memory Real-Time Graph

Note: Protocol and interface utilization percentages are calculated using deltas and therefore require two polling periods to be accurate.

Figure 3-35 Health Monitor Functionality Overview

Using the Health Monitor

To use the Health Monitor window, perform the following steps:

Step 1: Click on a Cisco network device.

While you are clicking on the device, pull down the Glyph menu and pull over to the Tools submenu. Continue to pull the Tools menu to the right to show the next level menu display. Select **Health Monitor**.

The message window shown in Figure 3-36 appears while the Health Monitor gathers information.

Figure 3-36 Health Monitor Message Window

If you want to quit, click on the **Quit** button.

If you do not quit, the Health Monitor window appears.

Step 2: Graph a device's memory usage by clicking on the **Free Memory** button and pulling down to the Real-Time Graphs icon.

The real-time graph appears seconds later. See Figure 3-37.

Figure 3-37 Free Memory Real-Time Graph for Cisco Device

The Cisco device *xyz.cisco.com* displays a free memory of almost 2 Mbytes.The start time of the real-time graph appears in the left bottom corner of the graph. The current poll time appears in the right bottom corner of the graph. The legend for this real-time graph includes the MIB object for free memory (freeMem).

Step 3: Graph CPU load data by clicking on the **CPU** button and pulling down to the Real-Time Graphs icon.

The real-time graph appears. See Figure 3-38.

Figure 3-38 CPU Load Real-Time Graph for Cisco Device

The Cisco device *abc.cisco.com* displays the device's CPU load. The legend includes the three MIB objects for *avgBusy1*, *avgBusy5*, and *busyPer*. The CPU busy percentage for one- and five-minute averages and for the last five-second period. The start time of the real-time graph appears in the bottom left corner of the graph. The current poll time appears in the bottom right corner of the graph.

Note: If a protocol button is grayed out, the protocol is not being used on this device. Therefore, there are no management capabilities on this protocol. If an interface button is grayed out, the interface might be down. When the interface comes back up, the button will become active.

Properties Window

Figure 3-39 illustrates the Properties window for the Real-Time Graphs application. Table 3-13 describes the components in this window.

Figure 3-39 Properties Window for Real-Time Graphs

Table 3-13 Properties Window Components

Component	Subcomponent	Description
Polling Frequency	Polling Interval Slider	Changes the polling rate by clicking on the slider. The default is 15 seconds.
Free Memory Format	Bytes Kbytes	Toggles format of free memory from bytes to kilobytes
OK Cancel		Accepts changes and exits window. Cancels any changes and exits window.

Using Device Contacts

When you need to find an onsite network manager or support contact quickly, use the **Contacts** application on the SNM Glyph Tools menu. To enter contact information, access the Device Management application and enter the information using the Devices window. Refer to the "Device Management" chapter for instructions on entering device contact data.

Note: The Contacts application has no authority checking and therefore is open to all users with access to CiscoWorks.

Accessing Device Contact Data

As part of your fault management procedures, you may choose to use device contacts as your quick access tool to find your emergency contact person. Once you have entered the necessary information in the Contacts window you can access this important information through the SNM Glyph menu.

To access your device contact data, complete the following steps:

Step 1: Click on the device for which you need contact information.

Step 2: Select Contacts by pulling down on the device to access the Glyph menu. Continue to pull over to the right to select the Tools submenu. Then pull down to **Contacts**.

A Contacts browser window appears containing the contact data. See Figure 3-40.

Figure 3-40 Contacts Window

If you think a contact should have been associated with a device but is not located in the list, review the device contacts assignments in Device Management.

Step 3: When finished, close the contacts window. To quit, pull down the File menu and select **Quit**.

Note: If several names are available, use the **Search Forward** or **Search Backward** buttons in the window to search through the list or the scroller. The list will scroll in a loop. If you miss some information, keep scrolling until it reappears. If there are no contacts associated with the selected device, a message stating there are no contacts available will display.

Using the Log Manager as a Diagnostic Tool

The Log Manager application enables you to store, query, and delete messages gathered from Cisco Systems devices on the internetwork. These messages are stored in the database in one Log Manager file and viewed through the Log Manager window. Two daemons, device monitor and event logging, also forward SNM event/trap reports into the log file. The Log Manager centralized log file differs from SNM's log file because it is permanent and does not erase if CiscoWorks is exited.

Log Manager File

Cisco devices (routers, protocol translators, and terminal servers) can send messages directly to the Log Manager. If you have System Software Release 8.3 or earlier, refer to the *Router Products Configuration and Reference* publication for a description of error messages. If you have Release 9.0, refer to the *System Error Messages*.

CiscoWorks application programs such as Device Monitor report to the syslog daemon, which sends messages to the Log Manager file.

The functionality of the Log Manager application is illustrated in Figure 3-41.

Figure 3-41 Log Manager Overview

Syslog Daemon

The syslog daemon (*syslogd*) can receive messages from devices on the network. Cisco Systems devices can send error messages and information directly to syslogd. Messages are also generated by CiscoWorks application programs and then sent to syslogd.

Syslogd reads and logs messages into a set of files described by the configuration file */etc/syslog.conf*. Each message is one line. The message can be tagged with a priority setting indicating if the message needs to be logged and, if so, into which file it will be logged.

Nmslog File

During installation, CiscoWorks creates the *nmslog* file (or log manager file), and syslogd timestamps and places the collection of message, traps, and events in this file.

CiscoWorks Log Daemon

The CiscoWorks Log daemon (nmlogd*)* reads the *nmslog* file, formats the messages into fields, and forwards them to the Sybase server daemon. Nmlogd reads the */etc/syslog.conf* file when it starts up and whenever it receives a SIGHUP signal.

Nmlogd must be run only on the machine on which CiscoWorks is installed. This machine is called the log host. If you want to run CiscoWorks applications on another machine and you want to log events, you must customize your */etc/syslog.conf* file. Refer to "Syslog.conf File" later in this chapter.

For more information on nmlogd, refer to the man page **nmlogd** (8) online or in the "Manual Pages" appendix.

Sybase Server Daemon

The Sybase server daemon (dataserver) stores the formatted log messages in the CiscoWorks database. The messages can then be viewed by the CiscoWorks Log Manager application.

Log Message Priority Settings

Priorities are encoded as a *facility* and a *level*. The facility describes the part of the system generating the message. The Configuration Management application and Cisco devices are recognized as facility *local7*. Levels are described in the following paragraphs.

For Cisco devices, the levels from highest to lowest priority are as follows:

- LOG_CRIT (indicates a critical condition)
- LOG_ERR (error messages)
- LOG_WARNING (warning messages)
- LOG_INFO (informational messages)
- LOG_DEBUG (includes only messages that contain information on debugging procedures)

For any SNMP devices or devices that support syslogd, the following seven levels, listed from most severe to least severe, can be used:

- **emergencies**—System unusable
- **alerts**—Immediate action needed
- **critical**—Critical conditions
- **errors**—Error conditions

- **warnings**—Warning conditions (output from Cisco device **debug** commands are logged at this level)
- **notifications**—Normal but significant conditions
- **informational**—Informational messages only
- **debug**—Debugging messages

To select the type of priority messages you want to log and define where these messages should reside, refer to the instructions under "Syslog.conf File."

Syslog.conf File

In the */etc/syslog.conf* file, you can add lines to select what type of priority messages should be logged and where they should be logged.

Note: The priority specified in *syslog.conf* causes messages of that priority or higher to be logged.

For example, to send informational messages from Configuration Management application programs and from the Cisco routers (facility *local7*) to a file named */var/log/nmslog*, the CiscoWorks installation program adds the following line to the */etc/syslog.conf* file during installation:

```
local7.log_info; /var/log/nmslog
```

Refer to your *CiscoWorks Getting Started Guide* for more information.

To be able to log events at workstations other than the log host, you must enter the following line into the */etc/syslog.conf* file:

```
local7.info; @loghost
```

With this entry in the file, the event is sent to loghost by the local syslogd. The loghost syslogd program places the event in the *syslog* file that is read by nmlogd.

Caution: Do not edit or remove the *nmslog* file that is specified in the */etc/syslog.conf* file. Syslogd and nmlogd keep track of the file. Use the *logpurg* program instead. Refer to "Using the Automatic Log Purge Program" later in this section.

Refer to the UNIX man pages **syslogd**, **logger**, and **syslog** for further information on how to mark messages by facility and priority level.

Note: You must send a SIGHUP signal to syslogd and nmlogd after editing the */etc/syslog.conf* file. To send the SIGHUP signal, log in as root and enter the command **kill -HUP** *process id.*

Log Manager Window

Figure 3-42 illustrates the Log Manager window. Table 3-14 describes the components in this window.

Figure 3-42 Log Manager Window

Table 3-14 Log Manager Window Components

Component	Subcomponent	Description
File	Print	Prints the selected fields of the log message in the current browser.
	Save	Saves the window changes to file.
	Version	Displays the CiscoWorks version information for this application.
	Quit	Exits the current window.
Edit	Check All	Checks all Text check boxes.
	Clear All	Clears all data fields and removes checks from the check boxes. Also refreshes the log browser with the current log in database.
	Delete	Purges the selected messages.
	Delete All	Purges all messages in the browser.
	Find	Searches for the data marked in the check boxes.
Security	Privileges	Displays the current user's security privileges.
	Change User	Enables you to change your user ID in order to access this application.
Help		Provides help text on the current window.
Data Fields	Message ID	Message identification number.
	Time	The time the message was received by syslogd.
	Application	Application name.
	Text	Any text string in the log file.
	Device	Device or element name.
	Event	Event type.
	Sub Type	Subevent type. This field will always be set to NONE.
	Net Address	Network address.
	Protocol	Protocol name. This field will always be set to NONE.
	Sub System	Subsystem name. This field will always be set to NONE.
Delete		Purges the selected messages.
Delete All		Purges all messages in the browser.
Hit Count Indicator		Displays the message entry count in the log browser.

Accessing the Window

The Log Manager automatically collects network events designated in Device Monitor into the Sybase database. The Log Manager allows you to view messages saved in the database and to query groups of messages using any combination of ten criteria.

To access the Log Manager, perform the following steps:

Step 1: Select the Tools menu and pull down to **Log Manager**.

The Log Manager window appears.

Step 2: Browse through the Log Manager messages by using the scroll bars.

Refer to your SNM documentation set for more information on OPEN LOOK window features.

While in the Log Manager window, you can query for log messages, print log messages, delete messages, and set up an automatic log purging function. These functions are explained later in this chapter.

Querying the Log Manager

You can use any of the following methods to query the Log Manager for a particular message or set of messages:

- Click on any combination of the ten data field check boxes *and* enter a device name, network address, and so on as applicable, in the data entry fields. Specifying information in the data entry field further narrows the search for messages in the log file. Pull down the Edit menu to the **Find** command to find the applicable messages.

- Click on the Text check box and enter a simple expression to search for a particular message, or set of messages. Pull down the Edit menu to the **Find** command to find the applicable messages.

- Click on the Text check box and enter a complex expression to search for a particular message, or set of messages. Pull down the Edit menu to the **Find** command to find the applicable messages.

The **Check All** command checks all Text check boxes. The **Clear All** command clears all fields and removes checks from the check boxes. **Clear All** also refreshes the log browser with the log currently in the database. The **Delete** and **Delete All** commands purge unwanted messages from the Log Manager and allows you to enter a completely new query.

In Figure 3-43, the log files have been queried by the device name *altemus*.

Figure 3-43 Querying the Log Manager by Device Name

Event Types

The Event field indicates a type of status change that has occurred on the network. Refer to Table 3-15 for a list of CiscoWorks event types and definitions. This table also includes a description of which events under normal operating conditions are logged. Refer to RFC 1215, "*Defining SNMP Traps*," for detailed information on defining traps.

Table 3-15 Event Types Logged in the CiscoWorks Log Manager

Event Type	Description
TRAP	Received a trap message.
EventReport	Received an event message.
CiscoWorks	Received an CiscoWorks information or error message.

Caution: The Log Manager collects messages from all devices on your network map. If you set the event monitoring option in the Device Monitor, the Log Manager will log events for the devices you have specified. SNM listens to traps via the SNMP trap facility. If another process is accessing the facility, traps may not be logged. Refer to your *SunNet Manager 2.0 Reference Guide* for more information.

Check to see if the port is busy by invoking the following command:

```
hostname% netstat -an | grep 162
```

If the port is busy, you will see a line similar to the following output:

```
udp      0      0      *.162
```

In this example, 162 is the trap port. The **netstat** command does not determine which process is occupying the port. You need to determine this on a “best guess” basis. The process occupying the port can be any SNMP management program. To free the port, shut down the process currently accessing it.

Entering Simple Log Query Expressions

You can query the log messages more specifically by entering simple log query expressions. Figure 3-44 illustrates a simple expression created to find any messages that are numbered greater than 100.

Figure 3-44 Using a Simple Expression to Query the Log Manager

In Figure 3-44, the Message ID field in the Log Manager window is selected and the simple expression “>100” is entered into the field. When the **Find** command is applied, all messages numbered greater than 100 are listed in the window. The Hit Count field at the bottom of the window indicates that 57 messages were found with this query.

Note: If your hit count starts to affect the performance of your workstation, select more fields or redefine your expressions to narrow your target field of log messages to speed your search.

The syntax used for such a simple expression is:

```
comparison_operator <space> value
```

The comparison operator can be an =, >, <, >=, and so on. (These operators are described in detail in the “Transact-SQL Commands” section of the *Sybase Commands Reference* manual that is provided with CiscoWorks.)

Entering Complex Log Query Expressions

It is also possible to create more finite and detailed queries using complex expressions.

An example of using a complex expression to query a sequence of messages (numbered between 200 and 210) by the Message ID field is illustrated in Figure 3-45.

Figure 3-45 Using a Complex Expression to Query the Log Manager

In the following example, a complex expression is created to query all messages from any device name starting with D, and any device named ember, and any device named pile*:*

```
: LIKE “D%” OR @ = “ember” OR @ = “pile”
```

The following syntax rules are applied when creating these complex expressions:

- The expression starts with a colon (:) and a space.
- Operators must be prefaced with an at (@) symbol. The first operator is an exception to this rule. The @ replaces the actual field name in a real time SQL command.
- Each value in the expression must be enclosed in quotation marks (“ ”).The Message ID field is an exception to this rule; a number, rather than a string, is entered into the field.

Refer to the “Transact-SQL Commands” section of the *Sybase Commands Reference* manual for detailed information on how to construct complex expressions.

Printing the Log Manager

You can print the current Log Manager window information. For example, to print the query of messages with message ID numbers between 30 and 40, perform the following steps:

Step 1: First select the type of information from the current Log Manager window that you want to print out. In this example, the Message ID Time Stamp, and Event fields have been selected for printing.

Step 2: Select the File menu and pull down to the **Print** command.

The Print window appears. See Figure 3-46.

Figure 3-46 Print Window

Deleting Log Manager Messages

Messages in the Log Manager window are stored in a Sybase table called *ciscolog*. These messages can accumulate quickly, and the database can consume large amounts of hard disk space. In order to prevent your database from consuming too much disk space, you should delete unwanted Log Manager messages on a regular basis.

You can delete log messages from the Log Manager window in two ways. To delete the Log Manager messages directly from the Log Manager window, follow these steps:

Step 1: Select the message or messages in the Log Manager window that you want to delete.

You can also use a simple or complex expression to define which messages you want to delete.

Step 2: Select the **Delete** or **Delete All** command.

For example, if you select one file, and then click on **Delete**, a confirmation window appears to confirm the deletion.

Step 3: Click on **No** to cancel the command or **Yes** to delete the file.

The messages will be deleted from the Sybase database.

Deleting Messages Using isql

Log Manager messages can also be removed using the isql utility. The isql utility is used in the following situations:

- The Sybase transaction log runs out of space when you try to delete all messages in the Log Manger window.
- You need more flexibility in specifying which records to delete.
- You want to use a shell script to delete the log messages efficiently. A script can be run with **cron** to ensure that the log messages are removed at regular intervals.

Note: If the Sybase transaction log is filled up during the deletion of messages from the Log Manager window, you can resolve the problem by using the *$NMSROOT/etc/enlarge_nms* script to enlarge the transaction log. Instructions for using this script are provided in the section "Enlarging Disk Space Using a Shell Script" in the "Database Administration" chapter.

You can use the isql **truncate table** command or the **delete** command to remove log messages from the Log Manager window and the records from the Sybase table. The **truncate table** command removes *all* log messages in the Log Manager window, while the **delete** command removes only those messages you specify. The **truncate table** command uses less space in the transaction log.

The following steps explain how to use the isql **truncate table** command to delete all log messages from the Log Manger window and the *ciscolog* file:

Caution: The following procedure deletes *all* messages in the Log Manager window. Do not follow these steps if you want to delete the messages selectively.

Step 1: Enter the following command at the UNIX prompt (%):

```
% isql -Unmsuper -Ppasswd
```

Step 2: Enter the following commands in a sequence to clean the ciscolog file:

```
> truncate table ciscolog
> go
> quit
```

The isql utility also allows you to specify clauses for deleting the data in the *ciscolog* file using the **delete** command. For example, if you want to delete log records that are older than 3 days, perform the following steps:

Step 1: Enter the following command at the UNIX prompt (%):

```
% isql -Unmsuper -Ppasswd
```

Step 2: Enter the following commands to delete log records that are older than 3 days:

```
> delete ciscolog where datediff(day, timestamp, getdate()) > 3
> go
> quit
```

To automate the deletion of the log records, you can add these lines to a shell script that can be run manually or from cron. Refer to the manual pages on **cron** and **crontab** commands for more information.

An example of the contents of a sample shell script follows:

```
#!/bin/sh
$SYBASE/bin/isql -Unmsuper -Ppasswd <<EOF
delete ciscolog where datediff (day, timestamp, getdate ()) > 3
go
quit
EOF
```

Maintaining the Log Manager File

In addition to querying the log file messages, you can also delete them as necessary and set up an automatic log purging function to back up an old log file and create a new one.

Using the Automatic Log Purge Program

During the configuration of CiscoWorks, you may have responded **yes** to the prompt "Do you want to install the CiscoWorks log purging utility to be started by UNIX cron daemon?" If so, the utility automatically purges and backs up the log file every day.

Logpurg is a command utility that circulates the CiscoWorks *syslog* file. It renames the current CiscoWorks syslog file to the same path name with a day of the week, for example, nmslog.Tue. At midnight on Monday, an *nmslog.mon* file is created. At midnight Tuesday, an *nmslog.tue* file is created. The original log file is cleared out once a week—every Monday night at midnight. The new file overwrites the original file.

When you view the *nmslog* files in a directory by typing **ls -l** at the UNIX command line, the list includes the names of the *nmslog* files and the dates they were created. Following is a sample listing displayed by the **ls -l** command:

```
-rw-r--r--  1 root         4187 Mar  5 07:32 nmslog
-rw-r--r--  1 root        13108 Mar  4 18:48 nmslog.Fri
-rw-rw-rw-  1 root          226 Mar  3 14:26 nmslog.Thu
```

The date indicates the day when the file was created, and the name of the file (for example, *nmslog.Fri*) indicates the day when that *nmslog* file was closed.

If the **logpurg** command is issued with a path name, the process ID is also included, for example, *nmslog.Tue.1345*. **Logpurg** then creates a new log file and sends a SIGHUP signal to syslogd and nmlogd. After receiving a SIGHUP signal, syslogd and nmlogd configure the new log file to be used for current messages.

When it is started, **logpurg** gets the current syslog file pathname for */etc/syslog.conf* with facility name *local6* or *local7* and appends the filename with a weekday suffix.

Editing the Crontab File

You can customize the log purge utility by editing the crontab file.

For example, in the crontab file include a line similar to the following:

```
10 6 * * $NMSROOT/bin/purg $NMSROOT
```

Purg is a front end for the log purge program and sets up the $NMSROOT and SYBASE environment variables. 10 represents the minutes and 6 represents the hour. The two asterisks (*) represent the date and the day of the week. An asterisk (*) indicates select all days of the week. The cron program will execute this program at 6:10 a.m. every day.

If the nmlogd process is not running at the time, the old log file name is entered into *$TMPDIR/.nmlogdspool*. If you have more than seven files in *$TMPDIR/.nmlogdspool*, logpurg provides an error message similar to “Nmlogd died. Call your system administrator.” If you did not redirect the cron job output, the system will send this message to root.

In order to send signals to the *syslog* file, the log purge utility must be run as root.

Refer to the **cron**(1) and **crontab** man pages for more information on these commands.

Using Security Options

The Security menu enables you to change your user id if you need special access to the Log Manager application. You can also check your security privileges for your current user ID from this menu.

Refer to the “Using Security Manager Tools” application for more information on the security options.