Chapter 12

Monitoring the Network

An important part of network management involves monitoring trends on the network. By effectively monitoring network behavior, you can anticipate problems and correct them before they disrupt the network. Monitoring the network also provides you with a *baseline*, a sampling of how the network functions in its equilibrium state. This baseline is beneficial because if you experience a problem later, the changes in certain related parameters could lead you to a possible cause.

Chapter 12 targets the following objective in the Planning section of the Networking Essentials exam:

Test Objectives

- Select the appropriate hardware and software tools to monitor trends on a given network

Test Yourself

Stop! Before reading this chapter, test yourself to determine how much study time you will need to devote to this section.

1. An enhanced version of Network Monitor is included with __________.

   A. Windows NT

   B. Windows 95

   C. SMS

   D. SNMP

2. __________ keeps a record of the repair histories of network hardware.

   A. Network Monitor

   B. Event log

   C. Client Manager

   D. Nothing—you must do it yourself

Monitoring Network Trends

Monitoring the network is an ongoing task that requires data from several different areas. Some of the monitoring tools that keep watch on the network are discussed in other chapters. The purpose of this chapter is to bring these tools together so that you can view them in the context of an overall network monitoring strategy. The following list details some tools you can use to document network activities:

- Pencil and paper (very important in keeping records)
- A performance-monitoring tool, such as Windows NT's Performance Monitor
- A network-monitoring and protocol-analysis program—such as Windows NT's Network Monitor or the more powerful Network Monitor tool included with Microsoft's BackOffice System Management Server (SMS) package—or a hardware-based protocol analyzer
- A system event log, such as the Windows NT event log, which you can access through Windows NT's Event Viewer application.

Keeping Records

A detailed history of changes to the network serves as a tremendous aid in troubleshooting. When a problem occurs, the first thing you want to know is *what* has changed, and you can gather this information from a configuration management database.

The following list details some items your configuration records should include:

- Descriptions of all hardware, including installation dates, repair histories, configuration details (such as interrupts and addresses), and backup records for each server
- A map of the network showing locations of hardware and cabling details

- Current copies of workstation configuration files, such as CONFIG.SYS and AUTOEXEC.BAT files
- Service agreements and important telephone numbers, such as the numbers of vendors, contractors, and software support lines
- Software licenses to ensure that your network operates within the bounds of the license terms
- A history of past problems and related solutions

Monitoring Performance

Windows NT's Performance Monitor tool lets you monitor important system parameters for the computers on your network. Performance Monitor can keep an eye on a large number of system parameters, providing a graphical or tabular profile of system and network trends. Performance Monitor also can save performance data in a log for later reference. You can use Performance Monitor to track statistical measurements (called *counters*) for any of several hardware or software components (called *objects*). Some Performance Monitor objects that relate to network behavior are as follows:

- Network segment
- Server
- Server work queues
- Protocol-related objects, such as NetBEUI, NWLink, and NetBIOS
- Service-related objects, such as Browser and Gateway Services for NetWare

Of course, any system counter on a server machine—such as those classified under the Processor, Memory, or PhysicalDisk objects—could have implications for the network.

You should use Performance Monitor if you are experiencing problems, but you also should use Performance Monitor to log network activity when things are running smoothly. Logging normal network activity helps you establish a baseline, to which later measurements can be compared.

note

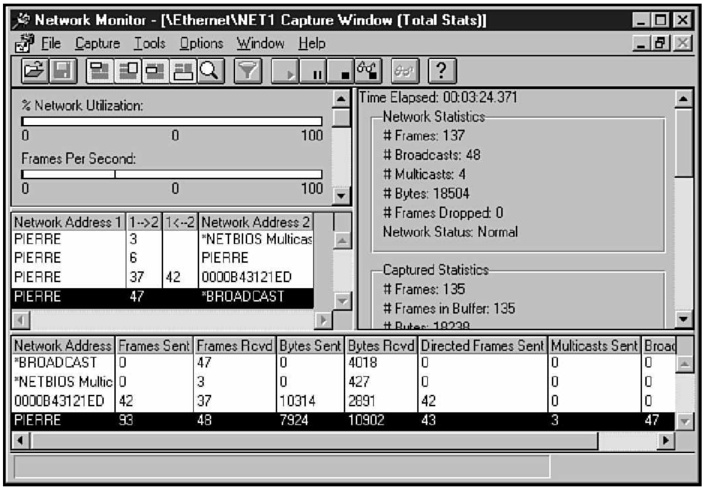
Exercises 12.2 and 12.3 at the end of this chapter provide you with a guided tour of Windows NT's Performance Monitor application.

Monitoring Network Traffic

Protocol analysis tools monitor network traffic by intercepting and decoding frames. Software-based tools, such as Windows NT Server's Network Monitor (see fig. 12.1), analyze frames coming and going from the computer on which they run. Network Monitor records a number of statistics, including the percent of network utilization and the broadcasts per second. In addition, Network Monitor tabulates frame statistics (such as frames sent and received) for each network address.

Figure 12.1

Windows NT Server's Network Monitor main screen.


Network Monitor - [\Ethernet\NET1 Capture Window (Total Stats)]
File Capture Tools Options Window Help
?

% Network Utilization:
0 0 100

Frames Per Second:
0 0 100

Time Elapsed: 00:03:24.371

Network Statistics
Frames: 137
Broadcasts: 48
Multicasts: 4
Bytes: 18504
Frames Dropped: 0
Network Status: Normal

Captured Statistics
Frames: 135
Frames in Buffer: 135
Bytes: 18238

Network Address 1	1-->2	1<--2	Network Address 2
PIERRE	3		*NETBIOS Multicas
PIERRE	6		PIERRE
PIERRE	37	42	0000B43121ED
PIERRE	47		*BROADCAST

Network Address	Frames Sent	Frames Rcvd	Bytes Sent	Bytes Rcvd	Directed Frames Sent	Multicasts Sent	Broad
*BROADCAST	0	47	0	4018	0	0	0
*NETBIOS Multic	0	3	0	427	0	0	0
0000B43121ED	42	37	10314	2891	42	0	0
PIERRE	93	48	7924	10902	43	3	47

An enhanced version of Network Monitor, which is included with the Microsoft BackOffice System Management Server (SMS) package, monitors traffic not just at the local system but also at other computers on the network.

For large networks, or for networks with complex traffic patterns, you might want to use a hardware-based protocol-analysis tool. A hardware-based protocol analyzer is a portable device that looks like a cross between a portable PC and a suitcase. The advantage of a hardware-based protocol analyzer is that you can carry it to strategic places around the network (such as a network node or a busy cabling intersection) and monitor the traffic at that point.

Some protocol analyzers are quite sophisticated. In addition to keeping network traffic statistics, they can capture bad frames and often isolate the source. They also can help determine the cause of bottlenecks, protocol problems, and connection errors. A hardware-based protocol analyzer is often a good investment for a large network because it concentrates a considerable amount of monitoring and troubleshooting power into a single, portable unit. For a smaller network, however, a hardware-based analyzer might not be worth the initial five-figure expense because less expensive software-based products perform many of the same functions.

Logging Events

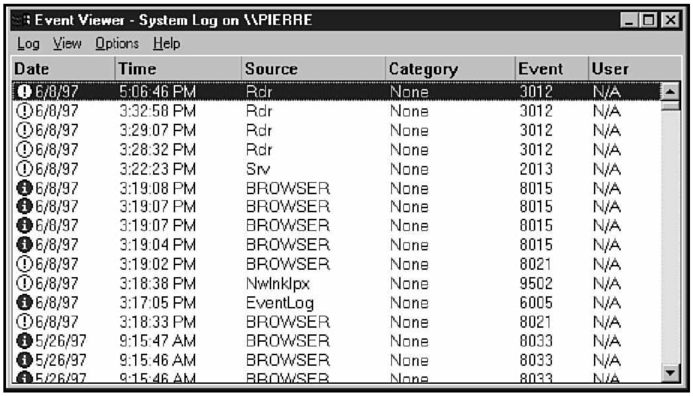
Some operating systems, such as Windows NT, have the capability to keep a running log of system events. That log serves as a record of previous errors, warnings, and other messages from the system. Studying the event log can help you find reccurring errors and discover when a problem first appeared.

Windows NT's Event Viewer application provides you with access to the event log. You can use Event Viewer to monitor the following types of events:

- **System events.** Warnings, error messages, and other notices describing significant system events. Examples of system log entries include browser elections, service failures, and network connection failures.

- **Security events.** Events tracked through Windows NT's auditing features. Refer to Chapter 8, "Managing and Securing a Microsoft Network."
- **Application events.** Messages from Win32 applications. If you're having a problem with an application, you can check the application log for an application-related error or warning messages.

Event Viewer is part of the Windows NT Server Administrative Tools group. To start Event Viewer, click on the Start button and choose Programs, Administrative Tools, Event Viewer. Figure 12.2 shows the Event Viewer main screen. Click on the Log menu to select the System, Security, or Application log.

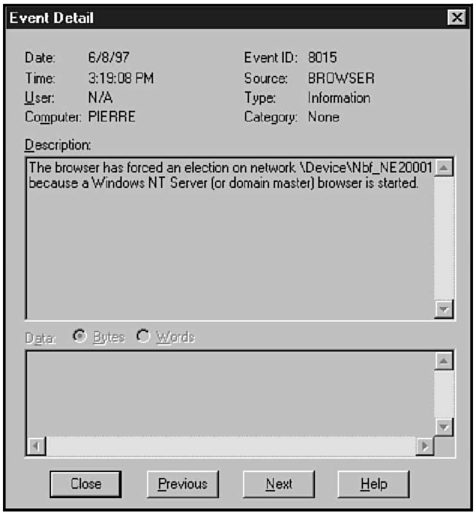


Date	Time	Source	Category	Event	User
⚠ 6/8/97	5:06:46 PM	Rdr	None	3012	N/A
⚠ 6/8/97	3:32:58 PM	Rdr	None	3012	N/A
⚠ 6/8/97	3:29:07 PM	Rdr	None	3012	N/A
⚠ 6/8/97	3:28:32 PM	Rdr	None	3012	N/A
⚠ 6/8/97	3:22:23 PM	Srv	None	2013	N/A
ⓘ 6/8/97	3:19:08 PM	BROWSER	None	8015	N/A
ⓘ 6/8/97	3:19:07 PM	BROWSER	None	8015	N/A
ⓘ 6/8/97	3:19:07 PM	BROWSER	None	8015	N/A
ⓘ 6/8/97	3:19:04 PM	BROWSER	None	8015	N/A
⚠ 6/8/97	3:19:02 PM	BROWSER	None	8021	N/A
⚠ 6/8/97	3:18:38 PM	NwInklpx	None	9502	N/A
ⓘ 6/8/97	3:17:05 PM	EventLog	None	6005	N/A
⚠ 6/8/97	3:18:33 PM	BROWSER	None	8021	N/A
ⓘ 5/26/97	9:15:47 AM	BROWSER	None	8033	N/A
ⓘ 5/26/97	9:15:46 AM	BROWSER	None	8033	N/A
ⓘ 5/26/97	9:15:46 AM	BROWSER	None	8033	N/A

Figure 12.2

The Event Viewer main screen.

If you double-click on a log entry in Event Viewer, an Event Detail dialog box will appear on your screen (see fig. 12.3). An Event Detail provides detailed description of the event.



Date: 6/8/97
Time: 3:19:08 PM
User: N/A
Computer: PIERRE
Event ID: 8015
Source: BROWSER
Type: Information
Category: None

Description:
The browser has forced an election on network \Device\Nbf_NE20001 because a Windows NT Server (or domain master) browser is started.

Figure 12.3

Event detail describing a system event.

Summary

This chapter reviewed some of the tools you can use to monitor network trends, including the following:

- Performance-monitoring devices
- Hardware- and software-based network-monitoring and protocol-analysis tools
- Event logs

This chapter also discussed the importance of keeping detailed written records of important network installations, configurations, and changes.

Exercises

Exercise 12.1: Using Network Monitor

Objective: Examine the main window display of Windows NT Server 4.0's Network Monitor application.

Estimated time: 15 minutes

1. If Network Monitor has been installed on your system, click the Start menu and choose Programs/Administrative Tools. Then choose the Network Monitor application from the Administrative Tools group and proceed to Step 4.

2. If Network Monitor hasn't been installed on your system, you must install it, along with a component called the Network Monitor Agent. Network Monitor and the Network Monitor Agent can be installed together by using the Control Panel Network application. Click the Start menu and choose Settings/Control Panel. Double-click the Network application and choose the Services tab.

3. In the Network application Services tab, click on the Add button. Choose Network Monitor and Agent from the Network Service list and click OK. Windows NT prompts you for the Windows NT installation disk. When the installation is complete, click OK to shut down your system and restart Windows NT. Then start the Network Monitor application, as described in Step 1.

4. Examine the four panes of the Network Monitor main screen (refer to fig. 12.1). The following list describes the four panes:

   - The Graph pane is located in the upper-left corner of the display. The Graph section includes five bar graphs describing network activity. Only two of the graphs are visible, as in figure 12.1; use the scroll bar to view the other three graphs.

   - The Session Statistics pane, which appears below the Graph pane, tracks network activity by session, showing the two computers in the session and the frames sent each way.

- The Total Statistics pane, which appears to the right of the Graph pane, lists such important statistics as the number of frames and the number of broadcasts. You can use the scroll bar to reach other entries that are not visible.
- The Station Statistics pane, which sits at the bottom of the window, shows statistics for frames listed by network address.

5. Pull down the Capture menu and choose Start. Network Monitor then starts monitoring the network.
6. Ping the Network Monitor PC from another computer on the network. (Go to the command prompt and type **Ping**, followed by the IP address on the Network Monitor computer—for example, ping 111.121.131.141.) Watch the Station Statistics pane at the bottom of the screen to see if any new information appears.
7. Experiment with sending files or other requests to or from the Network Monitor PC. Study the effect of network activity on the values displayed in the four panes of the Network Monitor main window.
8. When you are finished, pull down the Capture menu and click Stop to stop capturing data. Then exit Network Monitor.

Exercise 12.2: Creating a Chart in Performance Monitor

Objectives: Become familiar with the process of creating and reading a Performance Monitor chart. Understand the basic components of the Performance Monitor main window and the Add to Chart dialog box. Learn how to turn on disk performance counters using the *diskperf* command.

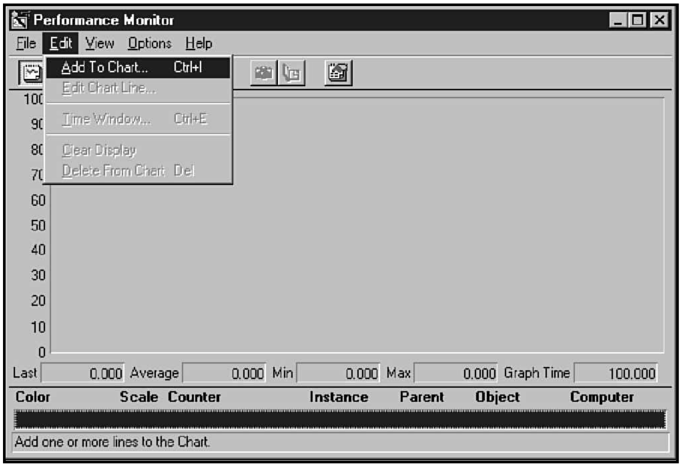
Estimated time: 25 minutes

1. From the Start menu, select Programs. Choose the Administrative Tools group and click Performance Monitor. The Performance Monitor main window appears on your screen.

continues

Exercise 12.2: Continued

2. Pull down the Edit menu and choose Add to Chart (see fig. 12.4.). The Add to Chart dialog box appears (see fig. 12.5). You can also invoke the Add to Chart dialog box by clicking the plus sign in the tool bar of the Performance Monitor main window.

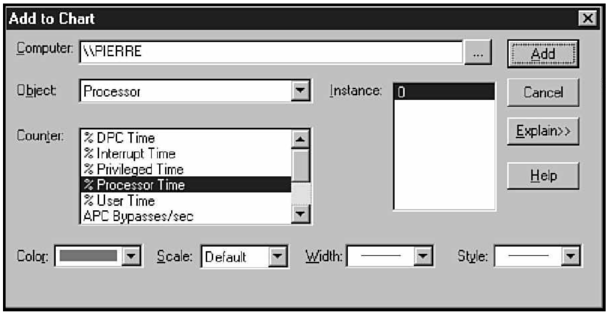


Last 0.000 Average 0.000 Min 0.000 Max 0.000 Graph Time 100.000

Add one or more lines to the Chart.

Figure 12.4

The Performance Monitor main window.



Computer: \\PIERRE

Object: Processor

Instance: 0

Counter: % Processor Time

Scale: Default

Figure 12.5

The Add to Chart dialog box.

3.a. The box labeled Computer at the top of the Add to Chart dialog box tells Performance Monitor which computer you want to monitor. The default is the local system. Click the ellipsis button to the right of the box for a list of computers on the network.

3.b. The box labeled Object tells Performance Monitor which object you want to monitor. As you learned earlier in this chapter, an object is a hardware or software component of your system. You can think of an object as a *category* of system statistics. Pull down the Object menu. Scroll through the list of objects and look for the Processor, Memory, PhysicalDisk, LogicalDisk, Server, and Network Segment objects described earlier in this chapter. Choose the PhysicalDisk object. If you have more than one physical disk on your system, a list of your physical disks will appear in the Instance box to the right of the Object box. The Instance box lists all instances of the object selected in the Object box. If necessary, choose a physical disk instance.

3.c. The box labeled Counter displays the counters (the statistical measurements) that are available for the object displayed in the object box. Scroll through the list of counters for the PhysicalDisk object. If you feel like experimenting, select a different object in the Object box. Notice that the new object is accompanied by a different set of counters. Switch back to the PhysicalDisk object and choose the %Disk Time counter. Click the Explain button on the right side of the Add to Chart dialog box. Notice that a description of the %Disk Time counter appears at the bottom of the dialog box.

3.d. Click the Done button in the Add to Chart dialog box. The dialog box disappears, and you see the Performance Monitor main window.

4. In the Performance Monitor main window, a vertical line sweeps across the chart from left to right. You may also see a faint colored line at the bottom of the chart recording a %Disk Time value of 0. If so, you haven't enabled the disk performance counters for your system. (If the disk performance monitors are enabled on your system, you should see a spikey line that looks like the readout from an electrocardiogram. You're done with this step. Go on to step 5.)

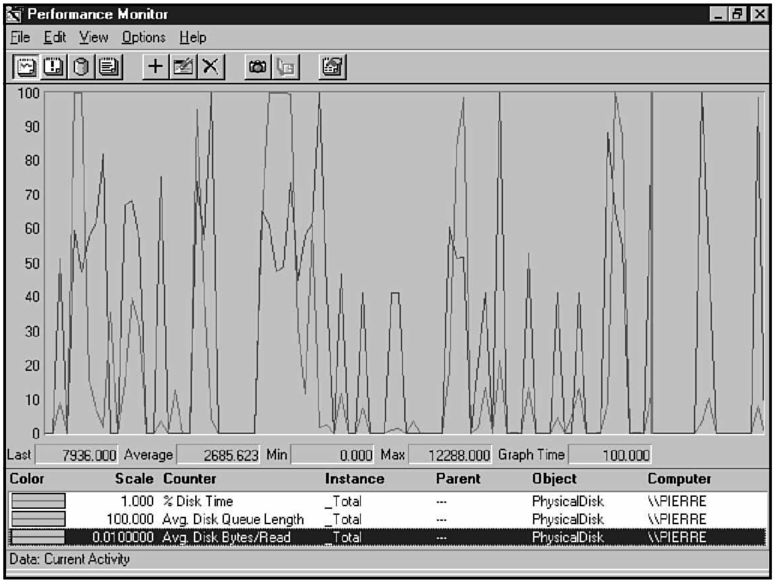
   If you need to enable the disk performance counters, click the Start button and go to the command prompt. Enter the command: **diskperf -y**. Then reboot your system and repeat Steps 1-4. (You don't have to browse through the object and counter menus this time.)

continues

Exercise 12.2: Continued

5. You should now see a spikey line representing the percent of time that the physical disk is busy reading or writing. Select Add to Chart from the Edit menu. Select the PhysicalDisk object and choose the counter Avg. Disk Queue Length. Click the Add button. Then choose the counter Avg. Disk Bytes/Read. Click the Add button and then click the Done button.

6. Examine the Performance Monitor main window. All three of the counters you selected should be tracing out spikey lines on the chart (see fig. 12.6). Each line is a different color. At the bottom of the window is a table showing which counter goes with which color. The table also gives the scale of the output, the instance, the object, and the computer.



Last 7936.000 Average 2685.623 Min 0.000 Max 12288.000 Graph Time 100.000

Color	Scale	Counter	Instance	Parent	Object	Computer
▬	1.000	% Disk Time	_Total	---	PhysicalDisk	\\PIERRE
▬	100.000	Avg. Disk Queue Length	_Total	---	PhysicalDisk	\\PIERRE
▬	0.0100000	Avg. Disk Bytes/Read	_Total	---	PhysicalDisk	\\PIERRE

Data: Current Activity

Figure 12.6

Displaying performance data.

7. Below the chart (but above the table of counters) is a row of statistical parameters labeled: Last, Average, Min, Max, and Graph Time. These parameters pertain to the counter that is selected in the table at the bottom of the window. Select a different counter and you see that some of these values change. The Last value is the counter value over the last

second. Graph time is the time it takes (in seconds) for the vertical line that draws the chart to sweep across the window.

8. Start Windows Explorer. Select a file (a graphics file or a word processing document) and choose Copy from Explorer's Edit menu. (This copies the file you selected to the clipboard.) Go to another directory and select Paste from the Edit menu. (This creates a copy of the file in the second directory.) Minimize Explorer and return to the Performance Monitor main screen. The disk activity caused by your Explorer session is now reflected in the spikes of the counter lines.

9. Pull down the Options menu and select Chart. The Chart Options dialog box appears on your screen (see fig. 12.7). The Chart Options dialog box provides a number of options governing the chart display. The Update Time section enables you to choose an update interval. The update interval tells Performance Monitor how frequently it should update the chart with new values. (If you choose the Manual Update option, the chart will update only when you press Ctrl+U or click Update Now in the Options menu.) Experiment with the Chart Options or click the Cancel button to return to the main window.

Figure 12.7

The Chart Options dialog box.

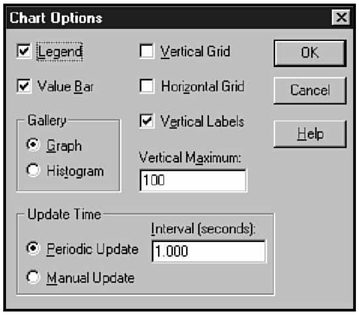


Chart Options

☑ Legend

☑ Value Bar

Gallery

● Graph

○ Histogram

□ Vertical Grid

□ Horizontal Grid

☑ Vertical Labels

Vertical Maximum: 100

Update Time

● Periodic Update

○ Manual Update

Interval (seconds): 1.000

10. Pull down the File menu. Choose Exit to exit Performance Monitor. Note that the Save Chart Settings and Save Chart Settings As options in the File menu enable you to save the collection of objects and counters you're using now so you can monitor the same counters later and avoid setting them

continues

Exercise 12.2: Continued

up again. The Export Chart option enables you to export the data to a file that you can then open with a spreadsheet or database application. The Save Workspace option saves the settings for your chart, as well as any settings for alerts, logs, or reports specified in this session. Learn more about alerts, logs, and reports in exercise 12.3.

Exercise 12.3: Performance Monitor Alerts, Logs, and Reports

Objectives: Become familiar with the alternative views (Alert view, Log view, and Report view) available through the Performance Monitor View menu. Log performance data to a log file.

Estimated time: 25 minutes

1. Click Programs in the Start menu and choose Performance Monitor from the Administrative Tools group. The Performance Monitor main window appears on-screen (refer to fig. 12.4).

2. Pull down the View menu. You'll see four options, as follows:

   - The Chart option plots the counters you select in a continuous chart (refer to exercise 12.1).

   - The Alert option automatically alerts a network official if the predetermined counter threshold is surpassed.

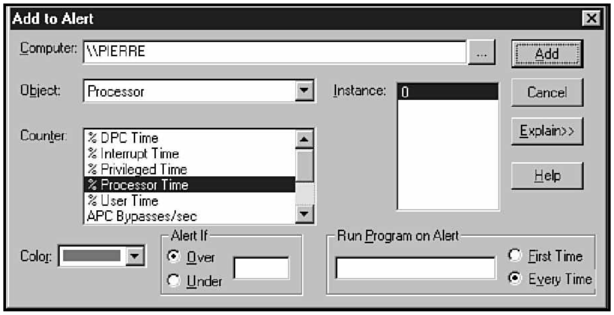
   - The Log option saves your system performance data to a log file.

   - The Report option displays system performance data in a report format.

   The setup is similar for each of these view formats. All use some form of the Add to Chart dialog box (refer to exercise 12.1). All have options that are configured through the first command at the top of the Options menu. (The first command at the top of the Options menu changes its name depending on the active view. It was the Chart option in exercise 12.1.)

3.a. Click the Alert option in the View menu.

3.b. Click the plus sign in the toolbar or choose Add to Alert from the Edit menu. The Add to Alert dialog box (see figure 12.8) is similar to the Add to Chart dialog box in figure 12.5 except for two additional items at the bottom of the screen. The Alert If box enables you to type in a threshold for the counter. The Over/Under radio buttons specify whether you want to receive an alert if the counter value is over or under the threshold value. The Run Program on Alert box lets you specify a command line that will execute if the counter value reaches the threshold you specify in the Alert If box. You can ask Performance Monitor to send a message to your beeper, to send you an e-mail message, or to notify your paging service.



Add to Alert

Computer: \\PIERRE

Object: Processor

Instance: 0

Counter:
% DPC Time
% Interrupt Time
% Privileged Time
% Processor Time
% User Time
APC Bypasses/sec

Color:

Alert If: ● Over ○ Under

Run Program on Alert: ○ First Time ● Every Time

Figure 12.8

The Add to Alert dialog box.

note

Don’t specify a batch file in the Run Program on Alert box. Performance Monitor uses Unicode format, which can confuse the command-prompt interpreter. (The < and > symbols, which are used in Unicode format, are interpreted as a redirection of input or output.)

3.c. The default object in the Add to Alert dialog box should be the Processor object. The default counter should be %Processor Time. Enter the value **5%** in the Alert If box and make sure the Alert If radio button is set to Over. In the Run Program on Alert box, type **SOL**. Set the Run Program on Alert radio button to First Time. This configuration tells Performance Monitor to execute Windows NT’s Solitaire program when the %Processor Time exceeds 5%.

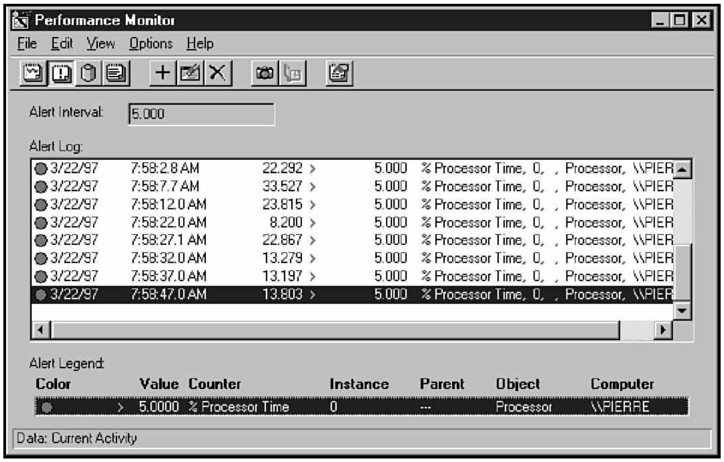
continues

Exercise 12.3: Continued

note

> If the Run Program on Alert radio button is not set to First Time, Performance Monitor will execute a new instance of Solitaire every time the %Processor Time exceeds 5%, which happens every time it executes a new instance of Solitaire. You'll probably have to close Performance Monitor using the X button or reboot to stop the incessant shuffling and dealing.

3.d. Click the Add button and then click the Done button. The Alert Legend at the bottom of the Alert window describes the active alert parameters. The Alert Log shows every instance of an alert (see fig. 12.9).



Alert Interval: 5.000

Alert Log:

```
● 3/22/97   7:58:2.8 AM    22.292 >   5.000  % Processor Time, 0,  , Processor, \\PIER
● 3/22/97   7:58:7.7 AM    33.527 >   5.000  % Processor Time, 0,  , Processor, \\PIER
● 3/22/97   7:58:12.0 AM   23.815 >   5.000  % Processor Time, 0,  , Processor, \\PIER
● 3/22/97   7:58:22.0 AM    8.200 >   5.000  % Processor Time, 0,  , Processor, \\PIER
● 3/22/97   7:58:27.1 AM   22.867 >   5.000  % Processor Time, 0,  , Processor, \\PIER
● 3/22/97   7:58:32.0 AM   13.279 >   5.000  % Processor Time, 0,  , Processor, \\PIER
● 3/22/97   7:58:37.0 AM   13.197 >   5.000  % Processor Time, 0,  , Processor, \\PIER
● 3/22/97   7:58:47.0 AM   13.803 >   5.000  % Processor Time, 0,  , Processor, \\PIER
```

Alert Legend:

Color		Value	Counter	Instance	Parent	Object	Computer
●	>	5.0000	% Processor Time	0	---	Processor	\\PIERRE

Data: Current Activity

Figure 12.9

The Performance Monitor alert log.

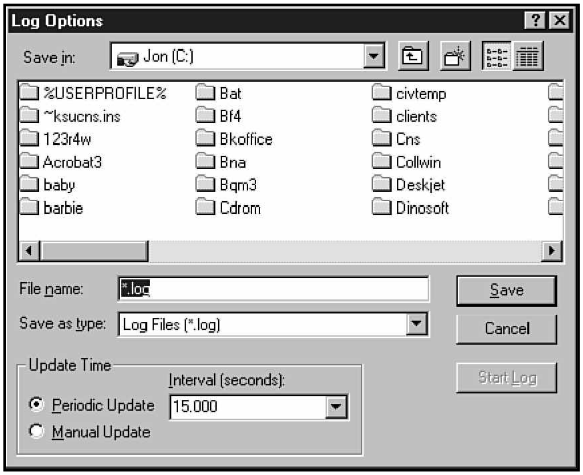
3.e. Make some changes to your desktop. (Hide or reveal the task bar, change the size of the Performance Monitor window—anything that will cause a 5% utilization of the processor.) The Solitaire program should miraculously appear on your screen. In a real alert situation, Performance Monitor would execute an alert application instead of starting a card game.

3.f. Pull down the Edit menu and select Delete Alert.

4.a. Pull down the View menu and select Log. Performance Monitor's Log view saves performance data to a log file rather than displaying it on the screen.

4.b. Pull down the Edit menu and select Add to Log. Notice that only the objects appear in the Add to Log dialog box. The counters and instances boxes don't appear because Performance Monitor automatically logs all counters and all instances of the object to the log file. Select the Memory Object and click Add. If you want, you can select another object, such as the Paging File object, and click Add again. When you are finished adding objects, click Done.

4.c. Pull down the Options menu and select Log. The Log Options dialog box appears on your screen (see fig. 12.10). The Log Options dialog box enables you to designate a log file that Performance Monitor will use to log the data. In the File name box, enter the name **exer2**. You also can specify an update interval. The update interval is the interval at which Performance Monitor records performance data to the log. The Manual Update radio button specifies that the file won't be updated unless you press Ctrl+U or select Update Now from the Options menu. Click the Start Log button to start saving data to the log. Wait a few minutes and then return to the Log Options dialog box and click the Stop Log button.



Log Options

Save in: Jon (C:)

File name: *.log

Save as type: Log Files (*.log)

Update Time

● Periodic Update — Interval (seconds): 15.000

○ Manual Update

Figure 12.10

The Log Options dialog box.

4.d. Pull down the View menu and switch to Chart view.

4.e. Pull down the Options menu and select Data From. The Data From dialog box enables you to specify a source for the

continues

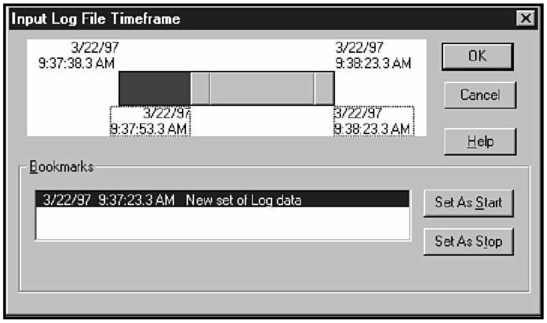
Exercise 12.3: Continued

performance data that appears in the Chart. Note that the default source is Current Activity. (That is why the chart you created in exercise 12.1 took its data from current system activity.) The alternative to the Current Activity option is to use data from a log file. Click the Log File radio button. Click the ellipsis button to the right of the log file window and select the exer2 file you created in step 4.c. Click OK.

4.f. Pull down the Edit menu and click Add to Chart. Click the down arrow to the right of the Object menu. Notice that your only object choices are the Memory object and any other objects you selected in step 4.b. Select the Memory object. Browse through the counter list and select Pages/sec. Click the Add button. Select any other memory counters you want to display and click the Add button. Click Done.

4.g. The log file's record of the counters you selected in 4.f appears in the chart in the Performance Monitor's main window. Notice that, unlike the chart you created in exercise 12.1, this chart does not continuously sweep out new data. That is because this chart represents static data from a previous, finite monitoring session.

4.h. Pull down the Edit menu and select Time Window. The Time Window enables you to focus on a particular time interval within the log file (see fig. 12.11). In this example (because you only collected data for a few minutes), the Time Window may seem unnecessary. If you collected data for a longer period, however, and you want to zero in on a particular event, the Time Window can be very useful. Set the beginning and end points of your time window by adjusting the gray start and stop sliders on the Time Window slide bar. The Bookmark section at the bottom of the dialog box enables you to specify a log file bookmark as a start or stop point. (You can create a bookmark by selecting the Bookmark option from the Options menu while you are collecting data to the log file or by clicking the book in the Performance Monitor tool bar.) Click OK to view the data for the time interval.



3/22/97
9:37:38.3 AM

3/22/97
9:38:23.3 AM

3/22/97
9:37:53.3 AM

3/22/97
9:38:23.3 AM

3/22/97 9:37:23.3 AM New set of Log data

Figure 12.11

The Performance Monitor Input Log File Timeframe dialog box, invoked by the Edit menu Time Window command.

5.a. Pull down the View menu and switch to Report view. Pull down the Options menu and select Data From. Switch the Data From setting back to Current Activity. Report view displays the performance data in a report rather than in a graphics format.

5.b. Select Add to Report from the Edit menu. Select the processor object and choose the %Processor Time, %Interrupt Time, and Interrupts/sec counters. (Hold down the Ctrl key to select all three and then click Add. Select the PhysicalDisk object and choose the %Disk Time, Avg. Disk Queue Length, and Current Disk Queue Length counters. Click the Add button. Select the Memory object and choose the Pages/sec, Page Faults/sec, and Available Bytes counters. Click the Add button. Click Done.

5.c. Examine the main report window. Performance Monitor displays a report of the performance data you specified in a hierarchical format, with counters listed under the appropriate object.

6. Select Exit in the File menu to exit Performance Monitor.

Review Questions

1. An advantage of hardware-based network monitoring tools over software-based tools is that __________.

   A. they are less expensive

   B. they are easier to use

   C. a hardware-based tool can also serve as a PC

   D. none of the above

2. Which tool would you use to determine if a Windows NT Server system displayed the same error message at the same time every day?

   A. Network Monitor

   B. Performance Monitor

   C. Event Viewer

   D. None of the above

3. Which tool would you use to determine if a Windows NT Server machine has enough RAM?

   A. Network Monitor

   B. Performance Monitor

   C. Event Viewer

   D. None of the above