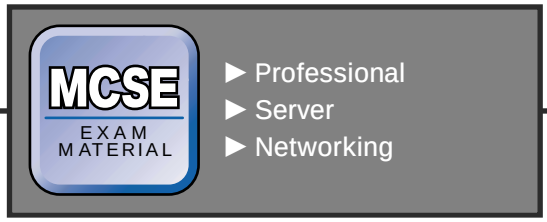

EXAM OBJECTIVES

Professional ▶

Exam 70-210

- Optimize and troubleshoot performance of the Windows 2000 Professional desktop.
  - Optimize and troubleshoot memory performance.
  - Optimize and troubleshoot processor utilization.
  - Optimize and troubleshoot disk performance.
  - Optimize and troubleshoot network performance.
  - Optimize and troubleshoot application performance.

Server ▶

Exam 70-215

- Monitor and optimize usage of system resources.
- Manage processes.
  - Set priorities and start and stop processes.
- Optimize disk performance.
- Monitor, configure, troubleshoot, and control access to files, folders, and shared folders.
  - Monitor, configure, troubleshoot, and control access to files and folders in a shared folder.

Networking ▶

Exam 70-217

- Manage and monitor network traffic.

CHAPTER

21

Monitoring, Optimizing, and Troubleshooting Performance

In a perfect world, we could simply configure our computers, walk away, and they would perform optimally all of the time. Unfortunately, this scenario is simply not reality. Windows 2000, as with any advanced operating system, requires monitoring, optimizing, and occasional troubleshooting in order to keep it working in peak condition. In this chapter, I'll examine the Windows 2000 processes and tools available to help you monitor and optimize it for its complex operations. In this chapter, I'll explain how to use System Monitor, Network Monitor, and Task Manager, how to monitor shared network folders, and how to optimize system components and troubleshoot performance problems.

Chapter Pre-Test

1. Which Windows 2000 tool replaces Windows NT 4.0's Performance Monitor?
2. System Monitor functions by using objects, instances, and _____.
3. Which System Monitor object would you use to examine the performance of your computer's hard disk?
4. What does Network Monitor capture?
5. You want to stop a process on your Windows 2000 Server computer. Which tool can you use to accomplish this?
6. Which Windows 2000 tool can be used to easily monitor shared network folders?
7. In most cases, what is the best solution to resolve poor memory performance on a Windows 2000 computer?
8. If your Windows 2000 computer's hard disk performance decreases over time, what is the most likely cause of the problem?

Monitoring Performance

As with any computer, your Windows 2000 computer's performance is based on many factors. Many people are under the mistaken impression that a fast CPU and plenty of memory will solve any performance problems they could possibly ever have. While it is true that your hardware drives much of your system's performance, a smart network administrator realizes that it is not only hardware and software that drive performance, but also how your computer uses that hardware and software.

In a nutshell, you monitor a computer's performance to determine how that computer is using its available resources. By monitoring performance, you can gain a clear picture of which components in your computer are performing optimally, and which components in your computer may have some trouble spots. By monitoring performance, you can learn what works well in your computer, and what doesn't work well in your computer. Then you can plan an appropriate course of action to correct any system problems that are degrading the performance of the Windows 2000 computer or your Windows 2000 network.

Unfortunately, performance tends to be a category of network administration that is ignored until there is a problem — this is a reactive approach. A better approach is a proactive one. Try to get in the habit of periodically monitoring different components in your computers to make sure that all hardware and software are working at their peak. This approach ensures the fastest performance, optimal server availability, and a way for you to solve computer and network problems proactively — before they ever begin.

Fortunately, the tools you may have used in Windows NT 4.0, such as Performance Monitor, Network Monitor, and Task Manager, return in Windows 2000 without too many changes. In the remainder of this chapter, I'll explain how to use these tools to solve performance problems on your Windows 2000 computers and on your Windows 2000 network.

Using System Monitor

System Monitor is a Windows 2000 tool that is used to monitor and chart the performance of system components in a Windows 2000 computer. System Monitor replaces Windows NT 4.0's Performance Monitor. In reality, System Monitor isn't much different than Performance Monitor. However, it is organized differently, and like most of the tools in Windows 2000, System Monitor functions as an MMC snap-in.

You can use System Monitor to:

- Identify performance problems and bottlenecks
- Determine current usage of system resources
- Track performance trends over time
- Predict future usage of system resources (capacity planning)
- Determine how system configuration changes affect system performance

System Monitor is installed, by default, on both Windows 2000 Professional and Windows 2000 Server computers. To access System Monitor, select Start ➪ Programs ➪ Administrative Tools ➪ Performance. Alternatively, you can Select Start ➪ Run, then type **Perfmon** and click OK. The Performance console, which hosts the System Monitor tool, is shown in Figure 21-1.

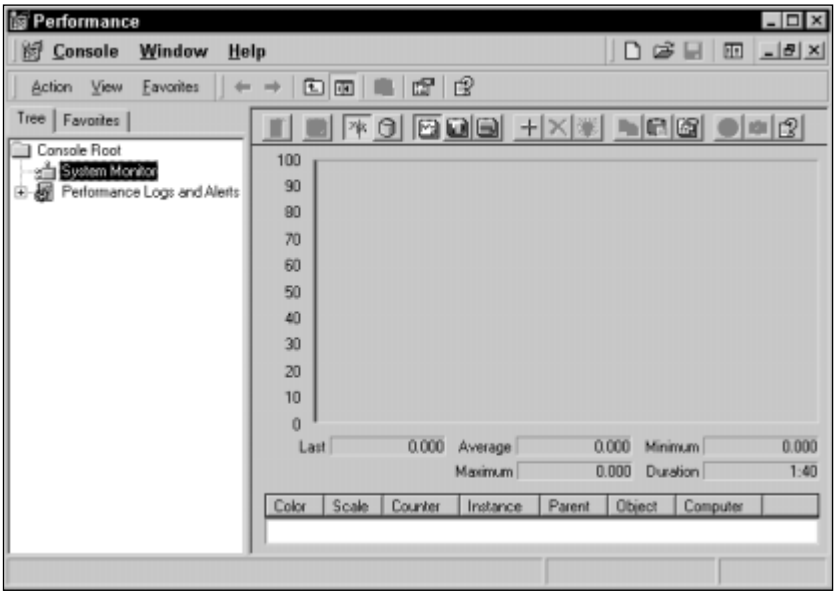

FIGURE 21-1 System Monitor user interface

In the following sections I'll show you how to configure and use System Monitor to examine the performance of your computer's system components.

System Monitor Objects, Instances, and Counters

System Monitor works by using objects, instances, and counters to gather performance data about the components in your Windows 2000 computer. You need to have a firm understanding of these three terms:

- **Object:** A system component, such as processor, memory, physical disk, and so on, is considered a System Monitor object.
- **Instance:** If a computer has more than one of a particular object, such as multiple processors or multiple physical disks, there is more than one instance of that object. Some objects, such as memory, do not have instances because there can't be more than one of that particular object.
- **Counter:** Each instance of an object can be measured in different ways. Each possible measurement of an instance is called a counter. Objects often have many different counters available. For example, when monitoring your physical disk, you can select from an assortment of counters. One measures disk reads, another measures disk writes, another measures disk time, and so on. Counters allow you to measure the performance of various aspects of objects.

TIP

Many BackOffice products, such as Systems Management Server, Proxy Server, Exchange, SQL Server, and so on, add their own counters to System Monitor when they are installed. You can then use System Monitor to examine the performance of these products.

So, you have a lot of objects and even more counters to choose from. Which are the most helpful? And how do you know when you should use a particular object or counter? Table 21-1 lists the most common counters used to monitor the performance of memory, physical disk, network, processor, and application performance.

EXAM TIP

The exams are likely to have questions on using some of the System Monitor objects and counters described in Table 21-1. Study this table carefully before you take the exams!

TABLE 21-1 Commonly Used System Monitor Objects and Counters

Object	Counter	Description
Memory	Pages/sec	This counter measures how often data is written to and read from the paging file. I use this counter to obtain an overall view of how memory is utilized by Windows 2000. A consistently high number (greater than 5 to 6) indicates that the current amount of RAM may be insufficient for the computer.
Network Interface	Bytes Total/sec	This counter measures the total number of bytes sent to and received from the selected network adapter. On computers with a single network adapter, this counter is useful for measuring the total network utilization of this computer.
Paging File	% Usage	This counter measures the percentage of paging file utilization. A consistently high percentage for this counter (approaching 100%) may indicate that you should add RAM to the computer or enlarge the paging file. Enlarging the paging file will not speed up the computer—only adding RAM will do that.
PhysicalDisk	Avg. Disk Queue Length	This counter measures the average number of disk reads and writes waiting to be performed. A consistently high number (greater than 4 to 5) may indicate that a faster hard disk or hard disk controller, or a different disk configuration (such as a striped volume or RAID-5 volume) may be required for adequate system performance.
PhysicalDisk	% Disk Time	This counter measures the percentage of time the disk performs reads and writes. A consistently high number (a number approaching 100 percent) may indicate that a faster hard disk or hard disk controller, or a different disk configuration (such as a striped volume or RAID-5 volume) may be required for adequate system performance.

Object	Counter	Description
Process	% Processor Time	This counter measures the percentage of time that the processor in the computer is actively used by one or more threads associated with the selected program or process. This counter is useful for determining which applications or services in a computer are consuming the most processor time.
Processor	% Processor Time	This counter measures the percentage of time that the processor is actively used by processes other than the Idle process. (The Idle process is the time the processor spends waiting to be assigned tasks.) A consistently high number (a number approaching 100 percent) may indicate that a faster processor (or an additional processor) may be required for adequate system performance.
Server	Bytes Total/sec	This counter measures the total amount of network utilization of a Windows 2000 computer. Specifically, it measures the total number of bytes sent to and received from all network adapters in the Windows 2000 computer by the Server service. This measurement can be used to compare utilization of two similar servers for load balancing purposes. It can also be used in conjunction with other measurements to determine network segment utilization.
Thread	% Processor Time	This counter measures the percentage of time that the processor in the computer is actively used by the selected thread. This counter is useful for determining which thread within an application or service is consuming the most processor time.

Using System Monitor to Gather and View Performance Data

Now that you have a basic understanding of the System Monitor objects and their counters, you're ready to use the System Monitor tool. In this section, you'll learn how to start System Monitor and how to use this tool

to gather performance data about a Windows 2000 computer and view this data in a chart.

When System Monitor data is displayed in a chart, the chart presents performance activity in a graphical format. You can use a System Monitor chart to view current performance activity, or to view archived performance activity from a log file. When viewing current performance activity, a System Monitor chart provides you with real-time data as it occurs on your computer.

STEP BY STEP

USING SYSTEM MONITOR TO GATHER AND VIEW DATA IN A CHART

1. Select ➪ Start ➪ Programs ➪ Administrative Tools ➪ Performance.
2. In the right-pane, click the Add button on the tool bar (this button appears as a **+** sign).
3. The Add Counters dialog box appears, shown in Figure 21-2.

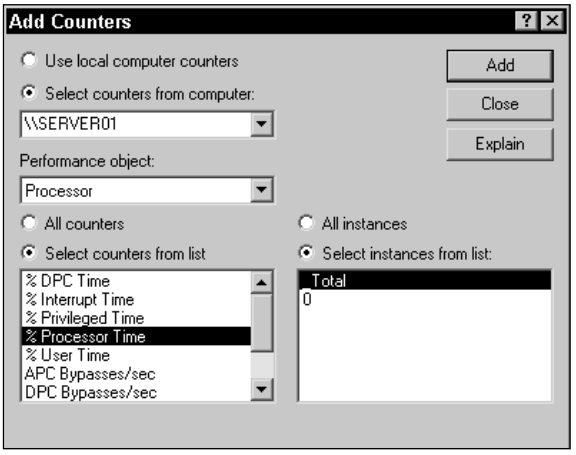

FIGURE 21-2 Selecting objects, counters, and instances

At the top of the dialog box, select from one of the two options:

- **Use local computer counters:** Select this option if you want to view performance data from the computer on which you are running System Monitor.
- **Select counters from computer:** Select this option if you want to view performance data from this computer, or from other computers on the network. If you select this option (which is selected by default), you must also select or type in a computer name (in the format `\\computer_name`) in the drop-down list box.

STEP BY STEP *Continued*

Next, select the object you want to monitor from the "Performance object" drop-down list box.

Then, select from the following two options:

- **All counters:** Select this option if you want to measure and view all counters associated with the object you selected.
- **Select counters from list:** Select this option if you want to measure and view only specific counters associated with the object you selected. If you select this option, also select the counters you want to use from the list box.

Finally, select from the following two options:

- **All instances:** Select this option if you want to measure and view all instances of the selected counter(s).
- **Select instances from list:** Select this option if you want to measure and view only specific instances of the counters you selected. If you select this option, also select the instance(s) you want to monitor.

TIP

When you're configuring this dialog box, click the Explain button at any time to view a detailed description of the highlighted object and counter combination. The description is displayed in the Explain Text dialog box that appears directly below the Add Counters dialog box.

When you finish selecting options for this object, click Add. Repeat this step to add additional objects and counters as necessary. When you finish selecting objects and counters, click Close.

4. System Monitor displays measurements of the objects and counters you selected in a chart in the right pane.

To maximize the size of the chart on your screen, select View ➪ Customize. Then clear the check box next to "Console tree" and click OK. Figure 21-3 shows a Performance Monitor chart with several objects and counters selected. Notice the Last, Average, Minimum, Maximum, and Duration boxes directly below the chart.

When you highlight any counter in the lower section of the dialog box, that counter's statistics are displayed in the Last, Average, Minimum, Maximum, and Duration boxes. Table 21-2 explains the statistics displayed in each of these boxes.

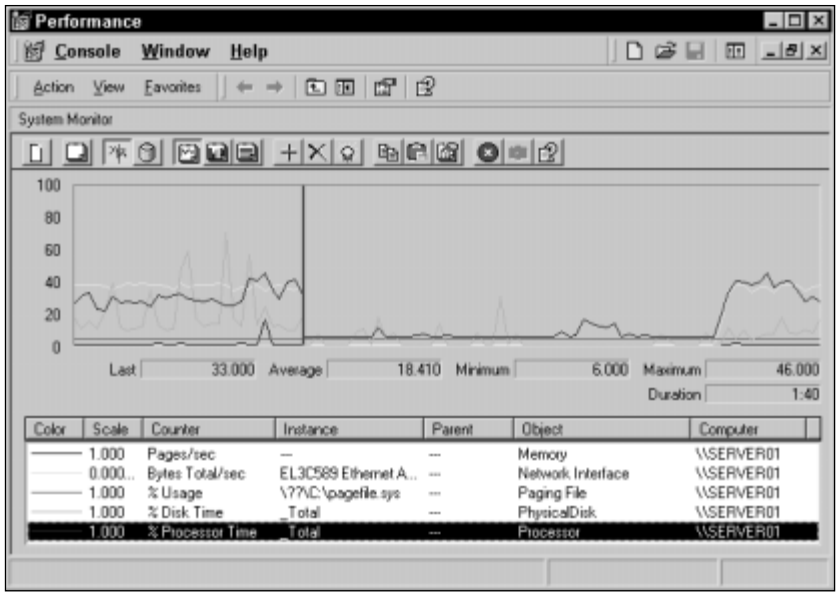

FIGURE 21-3 Viewing a System Monitor chart

TABLE 21-2 Statistics Displayed in a System Monitor Chart

Statistic	Description
Last	This is the most recent measurement of the counter.
Average	This is an average of the counter's measurement over the period of time represented by the chart.
Minimum	This is the lowest measurement of the counter during the period of time represented by the chart.
Maximum	This is the highest measurement of the counter during the period of time represented by the chart.
Duration	This is the number of minutes and seconds represented by the entire chart. This is the total amount of time it takes System Monitor to graph from one side of the chart to the other.

If you have difficulty determining which line on the chart represents the highlighted counter, you can press Ctrl + H to highlight that counter's line. Press Ctrl + H again to stop highlighting the counter's line on the chart.

In addition to viewing the data collected by System Monitor in a chart, you can also view this data in a report. To view data in a report, click the View Report button in the toolbar (this button appears as a writing tablet with lines on it, and is located to the left of the Add button).

TIP

To find out what each of the buttons in the toolbar can do, place your cursor over that button, and an identification box is displayed.

Figure 21-4 shows a System Monitor report.

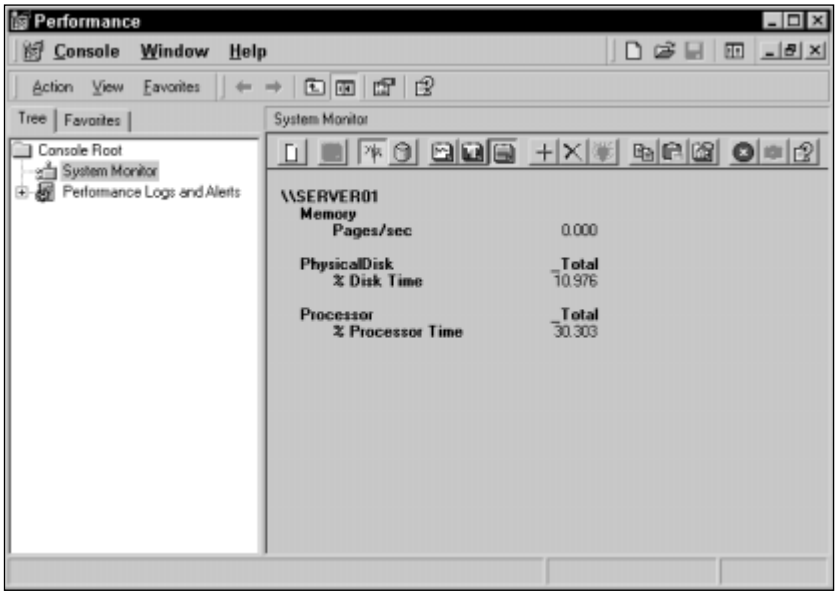

FIGURE 21-4 Viewing a System Monitor report

Finally, you can use System Monitor to view historical log file data as opposed to viewing a computer's current performance activity. You can create log files that can be viewed in System Monitor by using Performance Logs and Alerts, which is also a snap-in to the Performance MMC.

Using Network Monitor

Network Monitor is a Windows 2000 Server administrative tool that makes it possible for you to capture, view, and analyze network traffic (packets). Network Monitor doesn't ship with Windows 2000 Professional.

Network Monitor can be used to view network statistics, such as: percentage of network utilization, number of frames per second, number of broadcasts per second, and so forth. Network Monitor is useful for troubleshooting network problems, such as bottlenecks and protocol problems, as well as for determining how busy your network is.

Network Monitor is capable of capturing entire packets (also referred to as frames) from the network, and of analyzing the contents of each of these packets. You can save packets that are captured so you can study them later. It is important to keep in mind that the Network Monitor that ships with Windows 2000 is a scaled-down version designed to only capture packets sent to or from Windows 2000 Server computers. A more robust version of Network Monitor, that is capable of capturing all packets on the network segment, ships with Microsoft Systems Management Server.

Installing Network Monitor

Network Monitor is not installed by default during a normal Windows 2000 Server installation, so you'll need to install it by using Add/Remove Programs in Control Panel. Installing Network Monitor is very straightforward.

STEP BY STEP

INSTALLING NETWORK MONITOR

1. Select ➪ Start ➪ Settings ➪ Control Panel.
2. In the Control Panel dialog box, double-click Add/Remove Programs.
3. In the Add/Remove Programs dialog box, click Add/Remove Windows Components.
4. In the Windows Components dialog box, highlight Management and Monitoring Tools, then click Details.
5. In the Management and Monitoring Tools dialog box, select the check box next to Network Monitor Tools and click OK.
6. In the Windows Components Wizard dialog box, click Next.
7. When prompted, insert your Windows 2000 compact disc into your computer's CD-ROM drive and click OK. Close the Microsoft Windows 2000 CD dialog box. Windows 2000 installs Network Monitor.
8. In the Completing the Windows Components Wizard screen, click Finish.
9. Close Add/Remove Programs. Close Control Panel.

Using Network Monitor to Capture Packets

Once Network Monitor is installed, you can use it to capture network packets. Before I actually show you how to use Network Monitor, I want to introduce you to its main user interface, which is called the Network

Monitor Capture Window dialog box, or the Capture Window dialog box for short.

To access Network Monitor, select Start ➪ Programs ➪ Administrative Tools ➪ Network Monitor. The Capture Window dialog box is shown, after a capture has been performed, in Figure 21-5. (Until a capture is performed, no statistics appear in this dialog box. I'll explain how to perform a capture a little later in this section.)

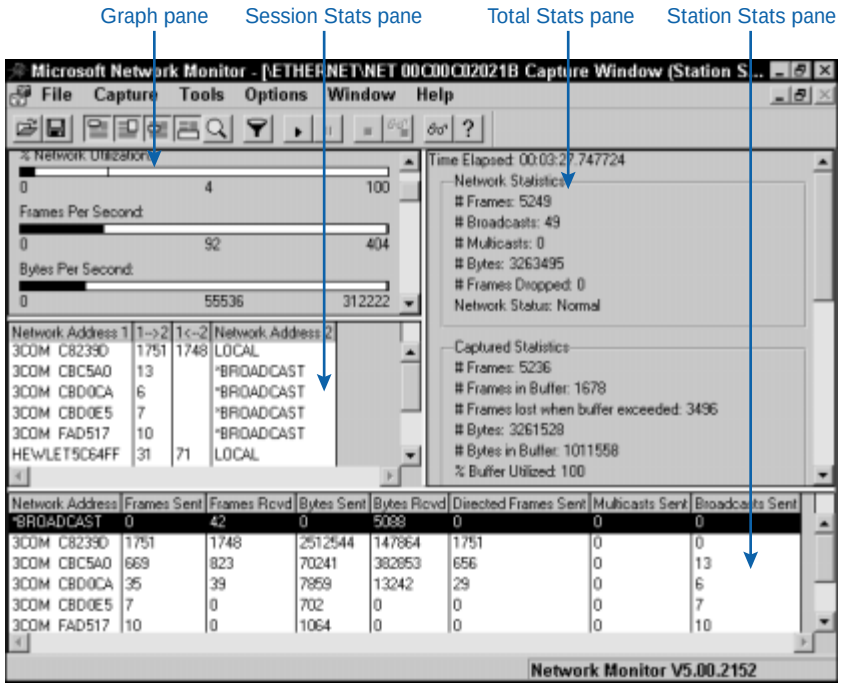

FIGURE 21-5 The Capture Window dialog box

As Figure 21-5 shows, the Capture Window dialog box has four panes: the Graph pane, the Session Stats pane, the Total Stats pane, and the Station Stats pane. You can use the Windows menu or the various buttons on the toolbar to configure which panes are displayed in this dialog box.

The Graph pane, which is the scrolling box located in the upper left corner of the Capture Window dialog box, displays five bar graphs. Each of these bar graphs depicts various network statistics, including % Network Utilization, Frames Per Second, Bytes Per Second, Broadcasts Per Second, and Multicasts Per Second.

The Session Stats pane, which is the scrolling list box located in the middle of the left side of the Capture Window dialog box, displays a summary

of packets transmitted between pairs of computers or network devices on the local network segment. Each computer or device in this pane is listed as either a network address or a computer name. Two statistics columns are shown between the pairs of network addresses/computer names. The first column displays the number of packets sent (during the capture period) from the computer or network device in the Network Address 1 column to the corresponding computer or device in the Network Address 2 column. The second column displays the number of packets sent from the computer or device in the Network Address 2 column to the corresponding computer or device in the Network Address 1 column.

The Total Stats pane, which is the scrolling list box located in the upper right corner of the Capture Window dialog box, displays five sections, each of which contains a different type of statistics. The five sections are: Network Statistics, Captured Statistics, Per Second Statistics, Network Card (MAC) Statistics, and Network Card (MAC) Error Statistics.

The Station Stats pane is the scrolling box located across the bottom of the Capture Window dialog box. This pane displays several statistics associated with each computer or network device that transmitted (or received) at least one packet to (or from) the Windows 2000 Server computer performing the capture during the capture period. Statistics shown include Network Address, Frames Sent, Frames Received, Bytes Sent, Bytes Received, Directed Frames Sent, Multicasts Sent, and Broadcasts Sent.

Now that you're familiar with the Capture Window dialog box and its panes, you're ready to perform a capture. Packets that you capture can be used for later analysis, and the process of capturing packets doesn't interfere with the packets reaching their intended destinations on the network.

STEP BY STEP

CAPTURING PACKETS

1. Select ➪ Start ➪ Programs ➪ Administrative Tools ➪ Network Monitor.
2. In the Microsoft Network Monitor Capture Window dialog box, select Capture ➪ Start.
3. Network Monitor continues to capture network packets until you stop the process. To stop a capture, select Capture ➪ Stop.

Configuring a Capture Filter Because a large number of packet statistics may be displayed in the Capture Window dialog box, you might want to use a capture filter to limit the type of network packets that Network Monitor will capture. By default, Network Monitor's capture filter is configured to capture *all* packets addressed to or sent by the Windows 2000 Server computer. However, you can change this default behavior so that only certain types of packets are captured. This feature is useful if you want to examine only certain types of network traffic. You can configure a capture filter so that:

- Only packets using certain protocols are (or are not) captured
- Only packets to or from specified computers or network devices are (or are not) captured
- Only packets containing specific byte patterns are captured
- Any combination of the preceding three

STEP BY STEP

CONFIGURING A CAPTURE FILTER

1. Select ➪ Start ➪ Programs ➪ Administrative Tools ➪ Network Monitor.
2. In the Microsoft Network Monitor Capture Window dialog box, select Capture ➪ Filter.
3. A Capture Filter dialog box appears, indicating that this version of Network Monitor can only capture packets sent to or from the local computer. Click OK.
4. The Capture Filter dialog box appears, as shown in Figure 21-6. Notice the default capture filter is displayed. In the next several steps I'll show you how to configure a filter to capture packets by protocol, address pairs, and byte patterns.
5. To configure a capture filter to capture packets by protocol, double-click SAP/ETYPE = Any SAP or Any ETYPE in the Capture Filter dialog box.
6. The Capture Filter SAPs and ETYPEs dialog box appears, as shown in Figure 21-7.

   Highlight the protocol(s) you want to exclude in the Enabled Protocols list box. Click Disable.

   Or, you can click Disable All to exclude all protocols, and then highlight the protocol(s) you want to include in the Disabled Protocols list box. Then click Enable.

   Click OK.
7. To configure a capture filter to capture packets by their associated computer name or network address, double-click (Address Pairs) in the Capture Filter dialog box.

STEP BY STEP *Continued*

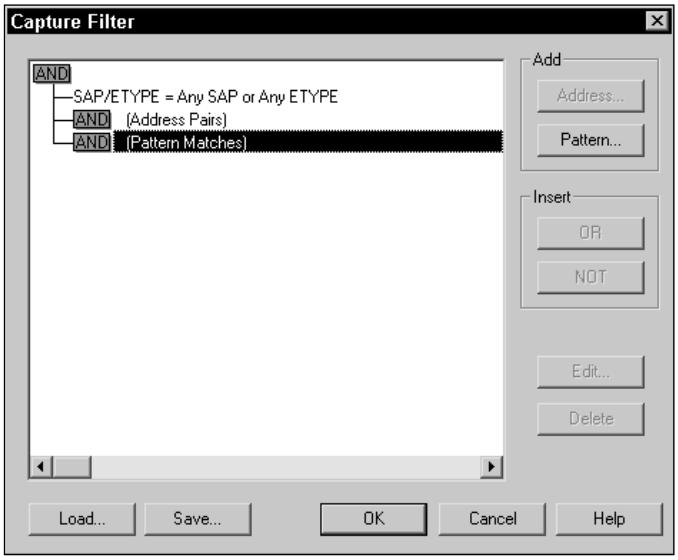

FIGURE 21-6 The Capture Filter dialog box

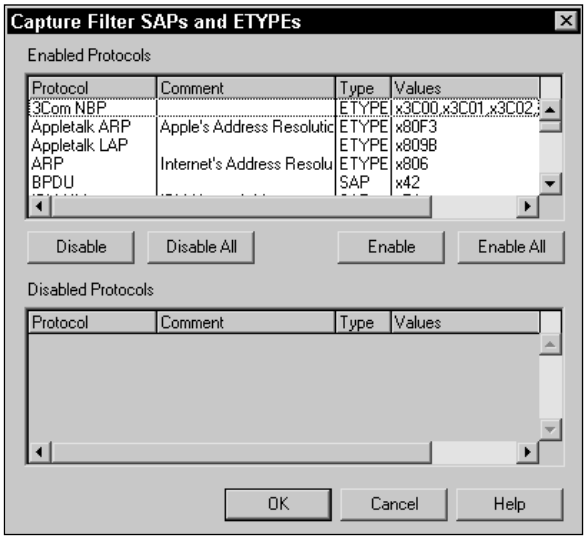

FIGURE 21-7 Configuring packets to be captured by protocol

STEP BY STEP *Continued*

8. The Address Expression dialog box appears, as shown in Figure 21-8. Note the Station 1 and Station 2 list boxes.

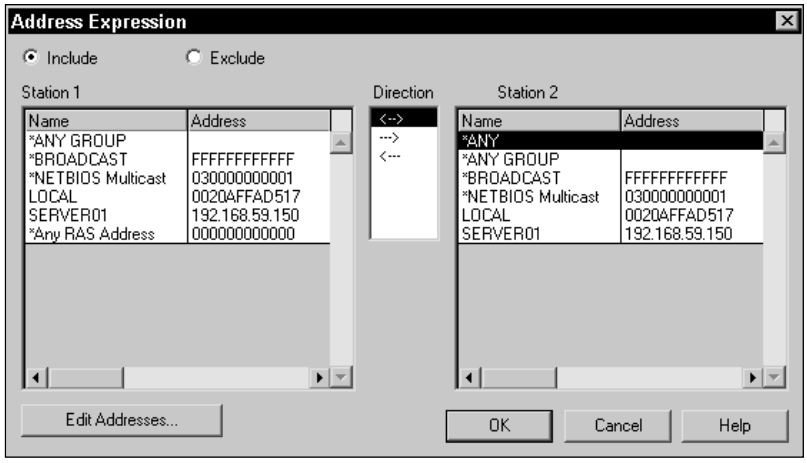

FIGURE 21-8 Configuring packets to be captured by network address or computer name

First, select the Include or Exclude option at the top of the dialog box, depending on whether you want to capture or exclude from capturing packets associated with a particular pair of computer names or network addresses.

Highlight a computer name or network address from the Station 1 list box. Then, highlight a direction arrow in the Direction list box to indicate whether the computer name or network address highlighted in the Station 1 list box is the packets' source address (--->), destination address (<---), or can be either the source or destination address (<-->).

Finally, highlight a computer name or network address from the Station 2 list box. Click OK. The new address appears in the Capture Filter dialog box. Network Monitor enables you to configure up to three address pairs in a single capture filter.

9. To configure a capture filter to capture packets by a specific byte pattern contained in those packets, double-click (Pattern Matches) in the Capture Filter dialog box.
10. The Pattern Match dialog box appears. Configure the Pattern and Offset (in hex) text boxes. Click OK.

STEP BY STEP *Continued*

CAUTION

Configuring a capture filter by byte pattern is normally done only by advanced users of Network Monitor. Detailed knowledge of packet construction is required to configure a pattern match filter.

11. The Capture Filter dialog box reappears. Click OK.

Saving Captured Data After you finish performing a capture, you can save the captured data to a file for later analysis if you like. This feature is helpful because you can gather a collection of packet captures over a period of time, then analyze them at a time that is convenient for you.

To save captured packets to a file, select File ➪ Save As in the Capture Window dialog box after you stop a capture. Type in a name for the capture and click Save.

To view the saved file at a later time, select File ➪ Open in the Capture Window dialog box, and then select the file you saved in the Open dialog box.

Using Network Monitor to View Captured Packets

Captured packets are of no use until you view them and interpret the statistics and information displayed. You can use two primary dialog boxes to view captured data in Network Monitor: the Capture Window dialog box and the Capture Summary dialog box. The view you choose depends on the type of information you seek.

The Capture Window dialog box (the Network Monitor main dialog box) displays general network activity statistics. This dialog box is useful for determining current network utilization, the type and number of packets being sent on the network, and which computers are generating (or receiving) the most network traffic. These statistics are useful for troubleshooting and trend analysis.

The Capture Summary dialog box displays a listing of all packets captured, and enables individual packet contents to be viewed and analyzed. This dialog box is useful for troubleshooting protocol and network adapter driver problems.

The following sections explain how to view and interpret captured data by using the Capture Window and Capture Summary dialog boxes.

Using the Capture Window Dialog Box The Capture Window dialog box is the main Network Monitor dialog box that was shown in Figure 21-5. As previously mentioned, this dialog box has four panes: the Graph pane, the Session Stats pane, the Total Stats pane, and the Station Stats pane. In this section I'll show you how to use this dialog box to perform some of the most common network analysis tasks on captured data.

One common task is determining current network utilization. To determine the current utilization of a network segment, start a Network Monitor capture, and then watch the % Network Utilization bar graph in the Graph pane *during the entire capture period*. This graph displays only the most recent one-second's worth of network activity, so you must view it during the entire capture period to get a feel for overall network utilization. A high number on the graph (any number consistently over 50%) may indicate that there is too much traffic on the network segment.

Another common task is determining which computer is sending or receiving the most of a specific type of network traffic. You can sort any of the columns in the Session Stats and Station Stats panes to determine precisely which computer is sending (or receiving) the most of a specific type of network traffic. For example, you can sort the Frames Sent column in the Station Stats pane to determine which computer on the network segment sent the most packets during the capture period. Similarly, you can sort the Broadcasts Sent column in the Station Stats pane to determine which computer sent the most broadcasts during the capture period. You can also sort the Frames Received column in the Station Stats pane to determine which computer received the most packets during the capture period. All the other columns can be sorted, as well, to determine which computer was responsible for generating the most bytes sent, most directed frames sent, most multicasts sent, and so forth. When you sort a column, Network Monitor displays the output in descending order, with the largest number appearing at the top of the column. To sort a column, right-click anywhere in the column and select Sort Column.

Using the Capture Summary Dialog Box To access the Capture Summary dialog box, in the Capture Window dialog box, select Capture ➪ Display Captured Data. Figure 21-9 shows the Capture Summary dialog box.

Notice the dialog box lists, by frame number, all of the packets captured by Network Monitor during the capture period.

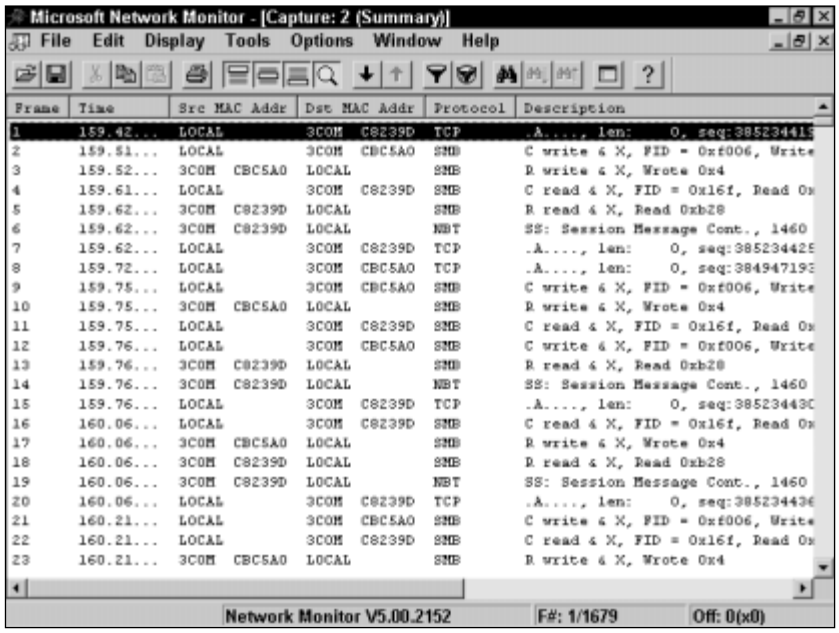

FIGURE 21-9 The Capture Summary dialog box

You can double-click any frame listed in this dialog box to obtain detailed information about the contents of that packet. For example, Figure 21-10 shows the packet details view for a specific packet. Notice the middle pane in the dialog box shows protocol decode information, and the lower pane in the dialog box shows, in hexadecimal, the entire contents of the packet.

If there are too many packets displayed in the Capture Summary dialog box, you can configure a display filter to limit the number of captured packets displayed. Configuring a display filter is very similar to configuring a capture filter.

Using Windows Task Manager

Windows Task Manager is a Windows 2000 graphical utility that can be used to monitor performance statistics, such as CPU and memory usage, to start and stop applications, and to change a process's base priority.

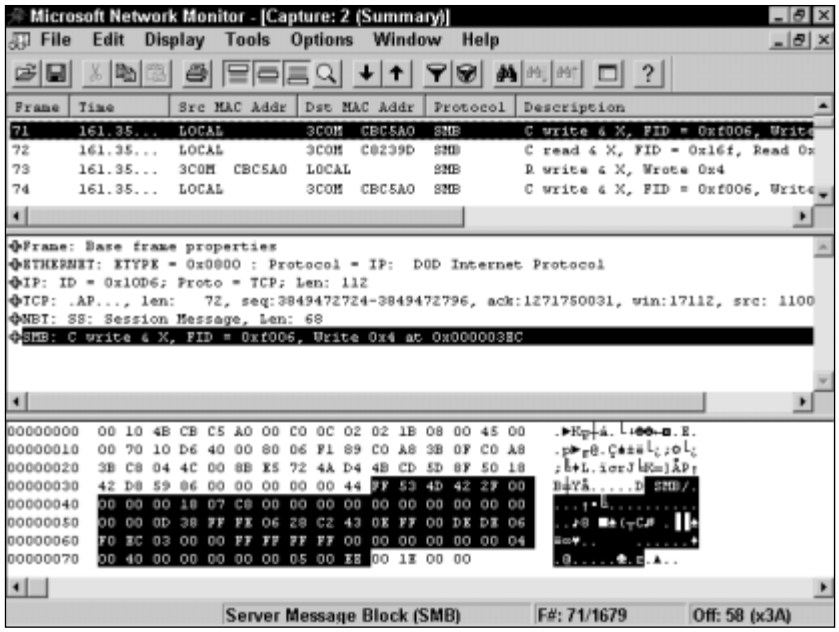

FIGURE 21-10 Viewing packet detail in the Capture Summary dialog box

You can access Windows Task Manager in several different ways:

- By pressing Ctrl+Shift+Esc
- By pressing Ctrl+Alt+Delete, and then clicking Task Manager
- By right-clicking a blank space on the taskbar (on the desktop), and then selecting Task Manager from the menu that appears
- By selecting Start ➪ Run, and then typing **taskmgr** in the Run dialog box

Figure 21-11 shows the Performance tab in Windows Task Manager. Notice the CPU Usage History and Memory Usage History sections.

In the following steps I'll show you how to use the Performance tab to monitor memory and processor usage. I'll show you how to use Windows Task Manager to start a process, stop a process, and change a process's base priority later in this chapter.

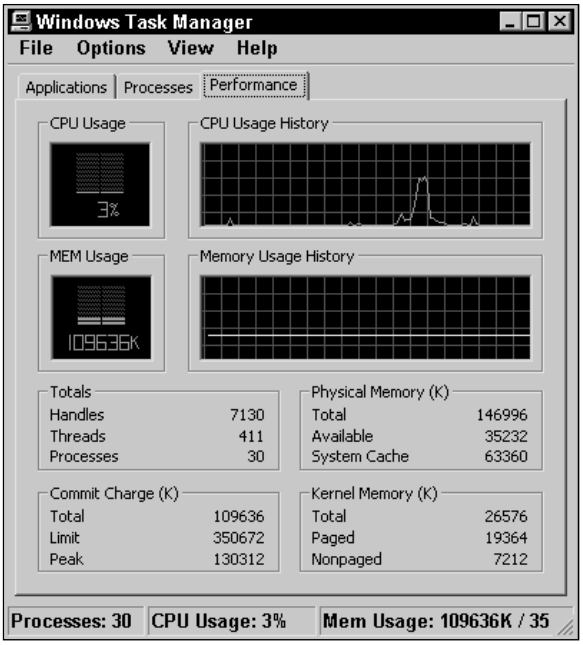

FIGURE 21-11 Windows Task Manager

STEP BY STEP

MONITORING MEMORY AND PROCESSOR PERFORMANCE BY USING TASK MANAGER

1. Press Ctrl+Shift+Esc.
2. In the Windows Task Manager dialog box, click the Performance tab if it is not displayed.
3. On the Performance tab, monitor the CPU Usage and Memory Usage statistics. You can also view the CPU Usage History and Memory Usage History graphs. When you finish monitoring performance statistics, exit Windows Task Manager.

Monitoring Shared Folders

Windows 2000 enables you to easily monitor shared network folders by using the Shared Folders tool in Computer Management. The Shared Folders tool enables you to:

- View a list of shared folders on the computer

- Monitor the number of computers currently connected to each shared folder
- View a list of specific users currently connected to shared folders on the computer
- Monitor the number of open files, by user
- Monitor the amount of time each user has been connected to the computer
- Stop sharing a folder
- Close open files in shared folders
- Disconnect users from the computer

I don't use this tool very often. However, it is extremely useful for closing a file in a shared folder when a client computer that was connected to the file has crashed. It's also useful for disconnecting users from shared folders prior to performing server maintenance tasks.

STEP BY STEP

MONITORING SHARED FOLDERS

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Computer Management. (Or, right-click My Computer and select Manage from the menu that appears.)
2. In the left pane of the Computer Management dialog box, click the + next to Shared Folders. Three subfolders appear under Shared Folders: `Shares`, `Sessions`, and `Open Files`.
3. In the left pane, highlight the `Shares` folder. In the right pane, a list of the shared folders on your computer is displayed, including the number of client computers connected to each shared folder. To stop sharing a folder, right-click the folder and select Stop Sharing from the menu that appears. Click OK to confirm the action you want to take. To modify the properties of a shared folder, right-click the folder and select Properties from the menu that appears.
4. In the left pane, highlight the `Sessions` folder. In the right-pane, a list of users that are currently connected to shared folders on your computer is displayed, as shown in Figure 21-12. Notice that the number of files each user has open and the amount of time the user has been connected to the computer are also displayed.

   To disconnect a user from all shared folders on the computer, right-click the user's name and select Close Session from the menu that appears. Click OK to confirm the action you want to take.

STEP BY STEP *Continued*

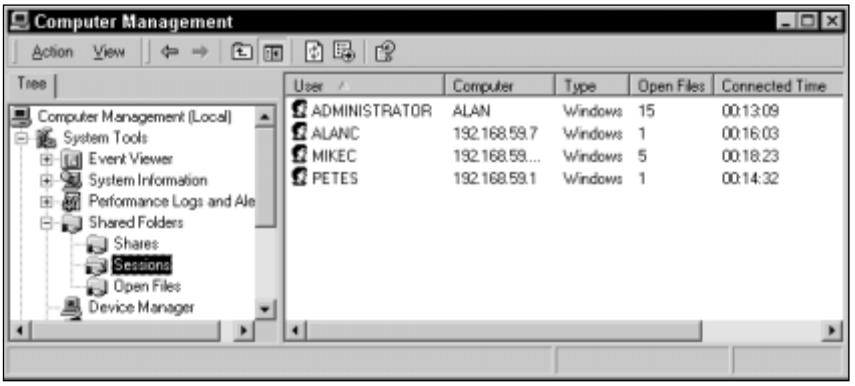

FIGURE 21-12 Monitoring user sessions

5. In the left pane, highlight the `Open Files` folder. In the right pane, a list of files currently open in shared folders on this computer is displayed. To close a file, right-click the file, and select Close Open File from the menu that appears. Click OK to confirm the action you want to take.
6. Close Computer Management.

Optimizing and Troubleshooting Performance

Where performance is concerned, optimizing and troubleshooting are two sides of the same coin. Optimizing is the process of configuring system or network components so they function at their peak. Troubleshooting is the process of determining which network or system components require optimization.

You can think of troubleshooting as diagnosing the performance problem, and optimizing as the solution. In many circumstances, optimization is performed because a problem has made itself known. However, you can take an proactive approach, develop an optimization plan, and resolve performance issues that could potentially become problems if no action is taken.

In the following sections I'll explore optimizing and troubleshooting performance of several key system components, including: memory, processor, disk, network, and applications.

EXAM TIP

You can expect the Windows 2000 exams—particularly the Professional exam—to have several questions on these optimizing and troubleshooting topics. I recommend you review the following sections carefully before taking the exams.

Optimizing and Troubleshooting Memory Performance

The single greatest cause of poor memory performance is a lack of RAM. You can't have too much RAM in your Windows 2000 computer. The more RAM you have, the more it can do in a shorter period of time. You should plan on regular, periodic RAM upgrades so your computer can meet the ever-increasing demands placed on it by operating systems, applications, and processes.

IN THE REAL WORLD

Operating systems and applications are constantly being updated and revised. Each new version seems to need more RAM. For example, Windows NT Server 4.0 requires a minimum of 16MB of RAM, while Windows 2000 Server requires a minimum of 256MB of RAM.

Adding RAM can reduce how often the computer reads or writes virtual memory pages to or from the paging file on the hard disk. This is called *reducing paging*. Because paging uses both processor time and disk time, when paging is reduced, the performance of the processor and the disk are also improved.

When RAM is added to the computer, Windows 2000 automatically increases the allocation of RAM made available to the disk cache. The disk cache temporarily stores user requested files from the hard disk in RAM. Because the disk doesn't need to be accessed when a file is retrieved from the cache, files in the cache are more quickly available to users than files on the disk. Thus, increasing the size of the cache can improve disk performance because the number of disk accesses is reduced.

In addition to installing more physical RAM, you can also optimize your paging file. The operating system uses the paging file to temporarily store memory data on the hard disk. As the computer runs low on physical memory, it uses the paging file to store memory pages, then recalls those pages from the hard disk as they are needed. To optimize your paging file, consider trying one or more of the following:

- Adding RAM, which lessens the use of the paging file
- Configuring the paging file so that its initial size and maximum size are equal — this prevents fragmentation of the paging file.
- Placing the paging file on the physical disk in your system that has the least amount of activity
- Placing the paging file on a striped volume
- Placing multiple, smaller paging files on multiple physical disks in your system
- Placing the paging file on any other partition than the boot partition

So, how do you know if you need more memory? First, Windows 2000 will let you know when it is running low on physical memory and will prompt you to close some of your applications. Additionally, you can use Windows Task Manager to see how much memory is being used, and how much of that memory is being paged. This information will give you a good look at how your computer uses memory and will help you know if you need to add more RAM. Finally, use System Monitor to chart the Memory-Pages/sec and Paging File-% Usage counters. When you examine the chart, if the Paging File-% Usage counter shows the usage of the paging file is approaching 100%, or if the Memory-Pages/sec counter is consistently greater than 5 to 6, then you probably need to add RAM.

Optimizing and Troubleshooting Processor Performance

As computer systems have evolved, the power and speed of processors have evolved as well. The processor in your Windows 2000 computer must be fast enough to handle the processing tasks placed on it, and if it can't, you will need to take some actions to resolve the problem. A point of warning, however, before you buy a new processor for a computer: make certain you have thoroughly examined your computer's memory. You may think

the problem is the processor, when in fact you don't have enough RAM to handle the processing jobs.

So, use System Monitor and Windows Task Manager to check both your processor and your memory, so you know exactly what the problem is. If you determine that your processor is too slow, you have a few decisions to make. First, you can simply upgrade the processor to a faster one. Or, you can add a processor so that your computer uses two, or you can keep your existing processor and remove some of the server's load by moving other processes or tasks to different servers.

Before upgrading your processor, take a good look at your entire computer. It may be time for a new computer, in which case, it would probably be a waste of money to buy a new processor if the entire computer needs to be replaced anyway.

Optimizing and Troubleshooting Disk Performance

Like other system components, physical disks may also need optimizing and troubleshooting. Normally, when there's a disk problem, users will notice a system slowdown when trying to read or write data to the hard disk. This can be caused by increased utilization of a slow hard disk, a slow hard disk controller, or a fragmented hard disk. You can use System Monitor to determine how the hard disk in your Windows 2000 computer is performing, and if your disk is, in fact, the bottleneck that is causing poor performance.

The more disks are used, the more likely they are to become fragmented. When disks are fragmented, it takes longer to read and write data to the disks, and users notice this slowdown. You can easily fix a fragmented disk by using the Windows 2000 Disk Defragmenter tool. You can start Disk Defragmenter by selecting Start ➪ Programs ➪ Accessories ➪ System Tools ➪ Disk Defragmenter. Consider periodically running Disk Defragmenter (once a week or so) on your hard disks to maximize disk performance by minimizing disk fragmentation.

Some older hard disks and hard disk controllers may simply be too slow to meet your current use requirements. If this is the case, an upgrade is probably in order. You can also implement other solutions, in addition to regular disk defragmentation, that can help disk performance:

- Configure a striped volume across two or more hard disks. Striped volumes improve read and write performance due to the way data is striped across the disks.

- Configure a RAID-5 volume across three or more hard disks. A RAID-5 volume dramatically improves read performance because the data is striped across multiple disks. Write speed is only slightly improved, because of the need to calculate parity information. In addition, a RAID-5 volume provides a measure of fault tolerance that is not provided by a striped volume.

EXAM TIP

You should know that mirrored volumes, while they are an effective fault tolerance solution, don't improve disk performance in Windows 2000.

Optimizing and Troubleshooting Network Performance

Network performance problems can be difficult to locate. Typically, poor network performance results when too many computers are sending too much network traffic on a network segment. You can think of the network segment as a highway and network packets as automobiles. When there are too many packets, the network becomes congested. Your task, then, is to determine whether too much network traffic exists.

As I explained earlier in this chapter, you can use both Network Monitor and System Monitor to examine network traffic trends on your Windows 2000 network.

If you determine that there is too much network traffic on one or more network segments, consider further segmenting that network segment by installing a router or switch.

Another type of network traffic problem occurs when users report slow network response from a server located on the other side of a WAN link. In this situation, consider these options:

- Move the server to the other side of the WAN link so client computers can access the server directly, without having to send network traffic across the WAN link.
- Add an additional server of the appropriate type (domain controller, DNS, DHCP, WINS, or global catalog) on the other side of the WAN link to service the client computers on that side of the link and to minimize WAN traffic.

For example, when users access a Windows 2000 domain controller for logon authentication across a WAN link (and slow server response time is reported), consider placing an additional domain controller on the same side of the WAN link as the client computers that need to access it. Placing the domain controller physically close to the client computers will improve server response time and reduce WAN link traffic.

Optimizing and Troubleshooting Application Performance

As a general rule, problems with application performance occur when too many processes are running, or when some processes are consuming too many system resources. You can use both System Monitor and Windows Task Manager to monitor the performance of a process. In addition, you can use System Monitor to monitor the performance of individual threads within a process.

As you consider troubleshooting and optimizing application performance, you need to understand that Windows 2000 manages processes based on their priorities. Windows 2000 uses process priorities to determine which applications (processes) receive the most processor time. A process priority (sometimes just called a priority) is a number between 0 and 31 that is assigned to an application when it is started. Applications that have a high priority receive more processor time than applications with a low priority. When an application is started in Windows 2000, it is assigned a base priority. Windows 2000 can dynamically raise and lower an application's priority based on changing conditions in the computer.

By default, most user applications are assigned a base priority of 8, the normal priority. A user application can be assigned a base priority between 0 and 15. A real-time or kernel mode application can be assigned a base priority between 16 and 31. You can change the base priority of an application, as the next section explains.

Starting Applications at Various Priorities

In Windows 2000, the `start` command is used to start applications at various base priorities. The `start` command can be used in batch files and from the command prompt. The `start` command can't be used in shortcuts to applications. Several switches are commonly used with the

Windows 2000 `start` command. These switches are listed and described in Table 21-3. To view a complete list of switches for the `start` command, at the command prompt, type `start /?` and press Enter.

TABLE 21-3 Commonly Used Windows 2000 start Command Switches

Switch	Description
`/low`	Starts the application with a base priority of **4**.
`/belownormal`	Starts the application with a base priority of **6**.
`/normal`	Starts the application with a base priority of **8**. This is the priority that is normally assigned to most user applications. Windows 2000 typically starts user applications with a base priority of 8 when no other priority is specified.
`/abovenormal`	Starts the application with a base priority of **10**.
`/high`	Starts the application with a base priority of **13**.
`/realtime`	Starts the application with a base priority of **24**. Applications started at the real-time base priority can slow the performance of the operating system itself. The real-time base priority should be used with extreme caution and is not recommended for most applications.
`/min`	Does not affect the base priority of an application. It starts an application in a minimized window. This switch can be used in conjunction with a priority switch and, if desired, either the `/separate` or `/shared` switch.
`/max`	Does not affect the base priority of an application. It starts an application in a maximized window. This switch can be used in conjunction with a priority switch and, if desired, either the `/separate` or `/shared` switch.
`/separate`	Does not affect the base priority of an application. It starts a Win16 application in a separate memory space.
`/shared`	Does not affect the base priority of an application. It starts a Win16 application in the Win16 shared memory space.

Using Windows Task Manager to Manage Processes

Another important part of optimizing and troubleshooting application performance is managing processes. You can use Windows Task Manager to manage the processes that are currently running on your Windows 2000 computer. This includes starting and stopping processes, and changing the base priority of processes.

STEP BY STEP

STARTING, STOPPING, AND CHANGING THE BASE PRIORITY OF A PROCESS

1. Start Windows Task Manager. (Press Ctrl+Shift+Esc.)
2. In the Windows Task Manager dialog box, click the Processes tab.
   - ▶ **To start a process,** select File ➪ New Task. In the Create New Task dialog box, type the name of the application, folder, or document that you want to start and click OK.
   - ▶ **To stop a process,** highlight the process you want to stop and click End Process. Then click Yes in the Task Manager Warning dialog box to stop the process.
   - ▶ **To end a process and all of its associated sub-processes,** right-click the process and select End Process Tree. Then click Yes in the Task Manager Warning dialog box to stop the processes.
   - ▶ **To change the base priority of a process,** right-click the process and select Set Priority. Then, select the base priority you want to assign to this process from the menu that appears. Options include: Realtime, High, AboveNormal, Normal, BelowNormal, and Low. Figure 21-13 shows the Set Priority menu.

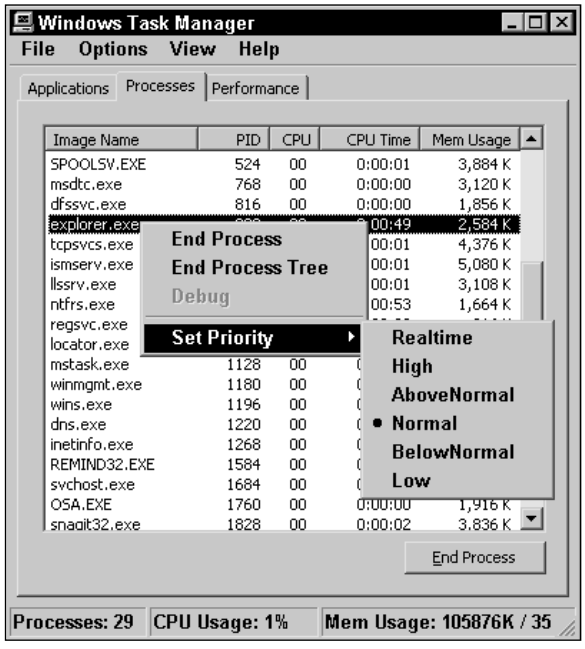

FIGURE 21-13 Setting a process's base priority

STEP BY STEP *Continued*

If a Task Manager Warning dialog box appears, click Yes to change the process's base priority.

3. When you finish managing processes, close Windows Task Manager.

Optimizing Performance of the Server

Optimizing your Windows 2000 Server computer enables you to get the most out of what you've got. There are four primary ways to optimize a server. You can optimize a server by configuring load balancing across multiple servers; disabling unused services, protocols, and drivers; scheduling server-intensive tasks for nonpeak hours; and optimizing the Server service.

Configuring Load Balancing

Configuring load balancing across multiple servers involves spreading server tasks among more than one server so that no one server is overburdened. Suppose that you have two servers that are primarily used for file and print services. One of these servers is functioning near peak capacity, while the other server is hardly being used. To improve overall server performance, consider moving a portion of the busy server's files to the other server. This will reduce some of the load on the busy server, and "balance the load" with the second server.

Disabling Unused Services

Another way to improve server performance is to disable unused services, protocols, and drivers. Each installed service, protocol, and driver uses processor time and memory space. Also, some services and protocols generate additional network traffic. If an installed service, protocol, or driver is no longer being used, consider removing the service, protocol, or driver; or, consider configuring the service, protocol, or driver to start manually instead of automatically.

Scheduling Server-intensive Tasks

Another way to improve server performance is to schedule large, server-intensive tasks to be performed during nonpeak hours. For example, if you

must update a large database or generate a large report on a daily basis, and it isn't critical that this task be done during business hours, consider scheduling the task to run after business hours (and before the tape backup is run for the night). If the task must be done during business hours, consider scheduling it to run during a period of lower activity, such as during a lunch hour.

Optimizing the Server Service

Finally, you can optimize the Server service for the type of tasks the server normally performs, and for the number of client computers that normally access the server. The Server service has the following four optimization options:

- **Minimize memory used:** Select this option when fewer than ten users will access the Windows 2000 Server computer at the same time, and when a user will sit at the server and use the server as his or her desktop computer.
- **Balance:** Select this option when fewer than sixty-four users will access the Windows 2000 Server computer at the same time. This option is also a good choice when the server is used for file and print services as well as by a distributed application that performs its own memory caching, such as Microsoft SQL Server.
- **Maximize data throughput for file sharing:** Select this option when more than sixty-four users will access the Windows NT Server computer at the same time, and when the server is primarily used as a file and print server. *This is the default option for Windows 2000 Server*, and is a good selection whenever the server functions primarily as a file and print server, even if there are fewer than sixty-four users.
- **Maximize data throughput for network applications:** Select this option when more than sixty-four users will access the Windows 2000 Server computer at the same time, and when the server is primarily used for a distributed application that performs its own memory caching, such as SQL Server. This is a good selection whenever the server functions primarily as an application server, even if there are fewer than sixty-four users. This is generally the best option for Windows 2000 domain controllers.

STEP BY STEP

CONFIGURING THE SERVER SERVICE

1. From the desktop, right-click My Network Places, then select Properties from the menu that appears.
2. In the `Network and Dial-up Connections` folder, right-click any Local Area Connection, then select Properties from the menu that appears.
3. In the Local Area Connection Properties dialog box, highlight File and Printer Sharing for Microsoft Networks, then click Properties.
4. The File and Printer Sharing for Microsoft Networks Properties dialog box appears, as shown in Figure 21-14. Notice the four optimization options.

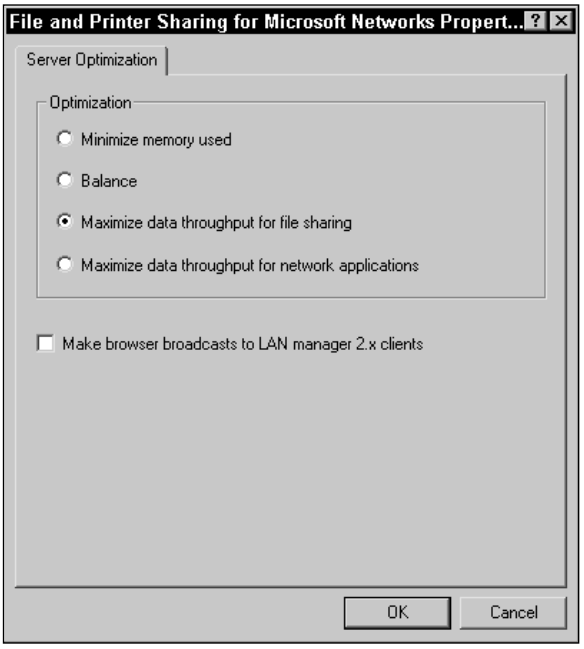

FIGURE 21-14 Optimizing the Server service

Select the option that will provide the best performance for your Windows 2000 Server computer. Click OK.

5. In the Local Area Connection Properties dialog box, click OK.
6. Close the `Network and Dial-up Connections` folder.

KEY POINT SUMMARY

This chapter introduced several important monitoring, optimization, and troubleshooting topics:

- System Monitor is a Windows 2000 tool that uses objects, instances, and counters to chart the performance of system components. Objects that are commonly monitored include: Memory, Network Interface, Paging File, PhysicalDisk, Process, Processor, Server, and Thread.
- You can use System Monitor to view current activity or to view historical log file data. Data can be viewed in a chart or in a report.
- Network Monitor is a Windows 2000 Server tool that enables you to capture, view, and analyze network packets. This tool is useful for troubleshooting network problems, such as bottlenecks and protocol problems.
- Packets captured by using Network Monitor can be saved and analyzed at a later time. This option allows you to make several captures and compare the captured data.
- Windows Task Manager is a Windows 2000 graphical utility that can be used to monitor performance statistics, such as CPU and memory usage. It can also be used to stop, start, and change the base priority of processes.
- You can use the Shared Folders tool in Computer Management to monitor shared folders. In addition, you can use this tool to close open files and disconnect users.
- The greatest cause of poor memory performance in a Windows 2000 computer is lack of RAM. In addition to optimizing the physical memory in a computer (RAM), you can also optimize your computer's paging file.
- Processors may need to be upgraded as a computer's workload increases. You can use System Monitor and Windows Task Manager to monitor the performance of your computer's processor.
- A common hard disk problem is fragmentation. Windows 2000 includes a defragmentation utility, called Disk Defragmenter, that you can use to resolve this problem. As with all system hardware, hard disks and hard disk controllers need to be upgraded periodically.

- If you determine, by using Network Monitor and System Monitor, that there is too much network traffic on a network segment, consider further segmenting that network segment by installing a router or a switch.
- Windows 2000 handles applications based on their priorities. You can use the `start` command to start applications at various base priorities. You can also use Windows Task Manager to start, stop, and change the base priority of a process.
- There are several ways to optimize a Windows 2000 Server computer, including: configuring load balancing across multiple servers; disabling unused services, protocols, and drivers; scheduling server-intensive jobs for nonpeak hours; and optimizing the Server service.

STUDY GUIDE

This section contains several exercises that are designed to solidify your knowledge about monitoring, optimizing, and troubleshooting Windows 2000, and to help you prepare for the Professional, Server and Networking exams:

- **Assessment questions:** These questions test your knowledge of the monitoring, optimization, and troubleshooting topics covered in this chapter. You'll find the answers to these questions at the end of this chapter.
- **Scenarios:** The situation-based questions in scenarios challenge you to apply your understanding of the material to solve a hypothetical problem. In this chapter's scenarios, you are asked to analyze performance situations, and to provide answers to the question or questions presented for each situation. You don't need to be at a computer to do scenarios. Answers to this chapter's scenarios are presented at the end of this chapter.
- **Lab Exercise:** These exercises are hands-on practice activities that you perform on a computer. The lab in this chapter gives you an opportunity to practice using several Windows 2000 tools to monitor and optimize performance.

Assessment Questions

1. You want to use System Monitor to see how much of the paging file on your Windows 2000 computer is being utilized. Which counter should you use?
   A. Paging File-% Usage
   B. Paging File-% Usage Peak
   C. Memory-Pages/sec
   D. Memory-Pool Paged Bytes

2. You want to use System Monitor to see how many disk reads and writes are having to wait to be serviced. Which PhysicalDisk counter should you use?
   A. % Disk Read Time
   B. Split IO/Sec
   C. % Idle Time
   D. Avg Disk Queue Length
3. You want to examine several counters to determine how applications are performing on your Windows 2000 computer. Which System Monitor object should you monitor?
   A. PhysicalDisk
   B. Process
   C. Processor
   D. Redirector
4. You want to use Network Monitor to capture network data, but you only want to capture packets that use a specific protocol. What should you do?
   A. Configure a network filter
   B. Configure a capture filter
   C. Configure a protocol filter
   D. Configure a packet filter
5. You want to determine which users are currently connected to shared folders on your Windows 2000 computer. In Computer Management, which subfolder of the Shared Folders tool should you use?
   A. `Shares`
   B. `Sessions`
   C. `Open Files`
6. Which base priority is assigned to most applications, by default?
   A. Realtime
   B. High
   C. Normal
   D. Low

7. You want to stop a process that is running on your Windows 2000 computer. Which tool should you use?
   A. Computer Management
   B. Windows Task Manager
   C. Windows Explorer
   D. Configure Your Server
8. What is the default optimization setting for the Server service on Windows 2000 Server computers?
   A. Minimize memory used
   B. Balance
   C. Maximize data throughput for file sharing
   D. Maximize data throughput for network applications

Scenarios

Monitoring, optimizing, and troubleshooting performance on your network can be complex tasks. For each of the following situations, consider the given facts and answer the question or questions that follow.

1. A Windows 2000 computer seems to be running slowly, especially when several applications are used at the same time. The hard disk drive indicator light is on almost all of the time, even when users are not accessing data from the hard disk.
   a. What is the most likely cause of the problem?
   b. What can you do to verify the cause of the problem?
   c. How can you resolve the problem and optimize the situation?
2. A user reports that tasks are taking longer than normal to complete on a particular Windows 2000 computer, especially when the computer has several tasks to complete at the same time.
   a. What is the most likely cause of the problem?
   b. What can you do to verify the cause of the problem?
   c. How can you resolve the problem and optimize the situation?

3. You notice that a particular Windows 2000 computer takes a long time to read information from its hard disk.
   a. What is the most likely cause (or causes) of the problem?
   b. What can you do to verify the cause of the problem?
   c. How can you resolve the problem and optimize the situation?
4. Several users report that server response time on a particular Windows 2000 network segment is slow.
   a. What is the most likely cause of the problem?
   b. What can you do to verify the cause of the problem?
   c. How can you resolve the problem and optimize the situation?
5. On a particular Windows 2000 computer, you notice that one specific application seems to run much slower than other applications.
   a. What is the most likely cause of the problem?
   b. What can you do to verify the cause of the problem?
   c. How can you resolve the problem and optimize the situation?
6. You want to optimize the hard disks on a particular Windows 2000 Server computer. What can you do to accomplish this?

Lab Exercise

Lab 21-1 Monitoring and Optimizing Performance

- ▶ Professional
- ▶ Server
- ▶ Networking

The purpose of this lab is to provide you with an opportunity to use several Windows 2000 tools to practice monitoring and optimizing the performance of your computer.

There are five parts to this lab:

- Part 1: Monitoring System Performance by Using System Monitor
- Part 2: Monitoring Network Performance by Using Network Monitor
- Part 3: Using Windows Task Manager to Manage Processes

- Part 4: Optimizing the Server Service
- Part 5: Monitoring Access to Shared Folders

Begin this lab by booting your computer to Windows 2000 Server and logging on as Administrator.

Part 1: Monitoring System Performance by Using System Monitor

In this part you use System Monitor to monitor the performance of your Windows 2000 Server computer.

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Performance.
2. In the Performance dialog box, in the toolbar in the right pane, click the Add button (which appears as a + sign).
3. In the Add Counters dialog box, select the "Use local computer counters" option. Select the Processor object from the "Performance object" drop-down list box. Then select the % Processor Time counter, and click Add.
4. Select the Memory object from the "Performance object" drop-down list box. Then select the Pages/sec counter, and click Add.
5. Select the Network Interface object from the "Performance object" drop-down list box. Then select the Bytes Total/sec counter, and click Add.
6. Select the PhysicalDisk object from the "Performance object" drop-down list box. Then select the % Disk Time counter, and click Add. Click Close.
7. View the System Monitor chart. Do you notice any problems with your computer's processor, memory, network, or disk performance?
8. Close System Monitor.

Part 2: Monitoring Network Performance by Using Network Monitor

In this part you install Network Monitor. Then you use Network Monitor to capture network packets and view network performance statistics.

1. Select ➪ Start ➪ Settings ➪ Control Panel.
2. In the Control Panel dialog box, double-click Add/Remove Programs.

3. In the Add/Remove Programs dialog box, click Add/Remove Windows Components.
4. In the Windows Components dialog box, highlight Management and Monitoring Tools, then click Details.
5. In the Management and Monitoring Tools dialog box, select the check box next to Network Monitor Tools and click OK.
6. In the Windows Components Wizard dialog box, click Next.
7. When prompted, insert your Windows 2000 compact disc into your computer's CD-ROM drive and click OK. Close the Microsoft Windows 2000 CD dialog box. Windows 2000 installs Network Monitor.
8. In the Completing the Windows Components Wizard screen, click Finish.
9. Close Add/Remove Programs. Close Control Panel.
10. Select Start ➪ Programs ➪ Administrative Tools ➪ Network Monitor.
11. In the Network Monitor – Select Default Network dialog box, click OK.
12. In the Select a network dialog box, click the + next to Local Computer. Then highlight the first network adapter shown in the list. Click OK.
13. Maximize the Microsoft Network Monitor dialog box. Maximize the Capture Window dialog box.
14. In the Microsoft Network Monitor Capture Window dialog box, select Capture ➪ Start. Wait five minutes. During the capture period, monitor the % Network Utilization bar graph. Then select Capture ➪ Stop.
15. Select Capture ➪ Display Captured Data. In the Capture Summary dialog box, double-click one of the packets that was captured, and view the packet detail.
16. Close the Microsoft Network Monitor Capture Summary dialog box. When prompted to save the capture, click No. If you are prompted to save the address database, click No.

Part 3: Using Windows Task Manager to Manage Processes

In this part you use Windows Task Manager to start and stop processes and to change a process's base priority.

1. Start Windows Task Manager. (Press Ctrl+Shift+Esc.)
2. In the Windows Task Manager dialog box, click the Processes tab.
3. On the Processes tab, select File ➪ New Task.
4. In the Create New Task dialog box, type **pinball**, then click OK.
5. Pinball opens on your desktop, behind Task Manager. Notice that `PINBALL.EXE` appears in the Windows Task Manager processes list. Highlight `PINBALL.EXE`, then click End Process.
6. A Task Manager Warning dialog box appears. Click Yes. Pinball is stopped and no longer appears in the processes list.
7. Select File ➪ New Task.
8. In the Create New Task dialog box, type **pinball** and click OK.
9. Right-click `PINBALL.EXE` in the processes list, and select Set Priority ➪ Realtime from the menus that appear.
10. In the Task Manager Warning dialog box, click Yes.
11. Minimize the Windows Task Manager dialog box and start a game of Pinball.
12. What happened? The Realtime setting has crashed your computer. Power off your computer and reboot it to Windows 2000 Server. Log on as Administrator.

Part 4: Optimizing the Server Service

In this part you use the `Network and Dial-up Connections` folder to optimize the Server service on a Windows 2000 domain controller.

1. From the desktop, right-click My Network Places, then select Properties from the menu that appears.
2. In the `Network and Dial-up Connections` folder, right-click any Local Area Connection, then select Properties from the menu that appears.
3. In the Local Area Connection Properties dialog box, highlight File and Printer Sharing for Microsoft Networks, then click Properties.
4. In the File and Printer Sharing for Microsoft Networks Properties dialog box, select the "Maximize data throughput for network applications" option. Click OK.
5. In the Local Area Connection Properties dialog box, click OK.
6. Close the `Network and Dial-up Connections` folder.

Part 5: Monitoring Access to Shared Folders

In this part you use the Shared Folders tool in Computer Management to monitor access to shared folders on your Windows 2000 Server computer.

1. Select Start ➪ Programs ➪ Administrative Tools ➪ Computer Management.
2. In the left pane of the Computer Management dialog box, click the + next to Shared Folders.
3. In the left pane, highlight the `Shares` folder. In the right pane, view the list of shared folders on your computer. Right-click the `Apps` folder, and select Properties from the menu that appears.
4. View the properties of the `Apps` folder. In the Apps Properties dialog box, click OK.
5. In the left pane, highlight the `Sessions` folder. In the right-pane, view the list of users that are currently connected to shared folders on your computer. This is probably an empty list, unless you're on a network.
6. In the left pane, highlight the `Open Files` folder. In the right pane, view the list of files currently open in shared folders on this computer. This is probably also an empty list.
7. Close Computer Management.

Answers to Chapter Questions

Chapter Pre-Test

1. System Monitor
2. System Monitor functions by using objects, instances, and *counters*.
3. The PhysicalDisk object is used to monitor hard disks.
4. Network Monitor captures network packets.
5. You can use Windows Task Manager to stop a process.
6. You can use the Shared Folders tool in Computer Management to monitor shared network folders.
7. Usually, adding RAM is the best solution for poor memory performance.

8. Fragmentation is a common hard disk problem that decreases hard disk performance.

Assessment Questions

1. **A.** The Paging File-% Usage counter is used to measure the percentage of paging file utilization.
2. **D.** The Avg Disk Queue Length counter is used to measure the average number of disk reads and writes waiting to be performed.
3. **B.** The Process object can be used to monitor application performance. (The Thread object is also useful for this task.)
4. **B.** Configure a capture filter to specify that only packets using a specific network protocol will be captured.
5. **B.** The `Sessions` folder lists the users currently connected to shared files and folders on the computer.
6. **C.** By default, most applications are assigned a base priority of Normal.
7. **B.** Windows Task Manager is used to start and stop processes.
8. **C.** The Maximize data throughput for file sharing setting is the default setting, and is appropriate for Windows 2000 Server computers that are functioning primarily as file servers. The Maximize data throughput for network applications setting is the preferred setting for domain controllers.

Scenarios

1. The problem in this scenario is most likely physical memory (RAM). The computer does not have enough memory to handle all of the application tasks. Use System Monitor to examine the Memory-Pages/sec and the Paging File-% Usage counters to confirm the memory problem. Your best and only practical solution is to add more RAM to the computer.
2. The most likely cause of this problem is the computer's processor. You should, however, rule out the possibility of insufficient RAM first. To verify the cause of the problem, view the System Monitor Memory-Pages/sec and the Processor-% Processor Time counters. You can resolve this problem by upgrading the processor, adding an additional processor, or removing some of the computer's workload.

3. In this scenario, the hard disk is either badly fragmented or is too slow. First, defragment the drive, then check the disk by using the System Monitor PhysicalDisk-% Disk Time and PhysicalDisk-Avg. Disk Queue Length counters. If the disk is too slow, you can replace it with a faster hard disk, or use a striped volume or RAID-5 volume.
4. In this scenario, there is probably too much traffic on the network segment. Use Network Monitor to monitor % Network Utilization on the segment. You can solve this problem by installing a router to further segment the network.
5. The most likely cause of this problem is that the application's base priority is set too low. Use Windows Task Manager or System Monitor to view the application's base priority. To resolve the problem, use Windows Task Manager to end unnecessary processes that may also be running. Then use Task Manager to raise the application's base priority.
6. To optimize hard disk performance, first run Disk Defragmenter on all disks, and implement a defragmentation plan so that disks are defragmented on a regular basis. Next, make certain that all hard disks and disk controllers are fast enough to handle the number of reads and writes required of them. Finally, you can further optimize servers that have two or more disks by configuring a striped volume, or, if you have three or more disks, by configuring a RAID-5 volume.

MCSE
EXAM
MATERIAL