MICROSOFT
TRAINING
AND CERTIFICATION

Microsoft Official
Curriculum

Module 14: Monitoring Resources and Performance

Contents

Microsoft

Instructor Notes

Presentation:
45 Minutes

Lab:
45 Minutes

This module provides students with the information and skills necessary to use System Information, Task Manager, Performance and Maintenance Tools, and Event Viewer to improve computer performance.

After completing this module, students will be able to:

- Determine important system information to assist in troubleshooting.
- Monitor computer performance by using Task Manager.
- Improve computer performance by using the tools in **Performance and Maintenance** in Control Panel.
- Monitor and interpret application and system events.
- Manage event logs.

Materials and Preparation

This section provides the materials and preparation tasks that you need to teach this module.

Required Materials

To teach this module, you need the following materials:

- Microsoft® PowerPoint® file 2272A_12.ppt
- Lab files, located on the Student CD in the Labfiles folder: App1-1.exe, App1-2.exe, App1-3.exe, App1-4.exe, App1-5.exe, Lab12.cmd, and Syslog.csv.

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the lab.
- Anticipate student questions and prepare answers to those questions.
- Thoroughly investigate Task Manager and the performance and maintenance tools in Control Panel so that you can effectively demonstrate their functions.

Instructor Setup for a Lab

This section provides setup instructions that are required to prepare the instructor computer or classroom configuration for a lab.

Lab 14A: Using Task Manager and Event Viewer

► **To prepare for the lab**

- Verify that students have access to needed lab files. Lab files are located on the Student CD in the Labfiles folder. The required files are: App1-1.exe, App1-2.exe, App1-3.exe, App1-4.exe, App1-5.exe, Lab12.cmd, and Syslog.csv.

Module Strategy

Use the following strategy to present this module:

- Determining System Information

  In this section, demonstrate how to gain access to system information. Explain how information in each of the four top-level categories (System Summary, Hardware Resources, Components, and Software Environment) can be used to aid in diagnostics or troubleshooting.

- Using Task Manager to Monitor System Performance

  In this section, demonstrate how to use and manipulate the information on each of the four Task Manager tabs. Ensure that students can define a process, and that they understand the effects of process priority. Discuss the Ctrl+Alt+Delete options, and when students might want to use those options to restrict access to Task Manager. Ensure that students understand the relationships between information on the various Task Manager tabs; for example, the CPU measure on the **Processes** tab and the CPU Usage on the **Performance** tab. Introduce the new **Networking** tab, and ensure that the students understand its functions.

- Using Performance and Maintenance Tools to Improve Performance

  In this section, demonstrate how to gain access to the Performance and Maintenance tools in the category view of Control Panel. Discuss each of the maintenance tools, and when to use them. Demonstrate how to configure visual effects, and emphasize that the default visual effect settings are based on the computer's capabilities. Next, discuss the advanced configuration options, and make sure that you explain the effects of each configuration change.

- Monitoring Event Logs

  In this section, first explain the concept of events. Emphasize that although there are three event logs, this module addresses only system events and application events. Explain that security events are the result of an audit policy, and because security is not usually locally audited on a computer running Microsoft Windows® XP Professional, security logs need not be addressed in this module. Demonstrate Event Viewer and show students how to search for and analyze events. Emphasize how to use the information gathered from analyzing events to troubleshoot problems. Finally, discuss the purposes of archiving and show students how to archive event logs.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Training and Certification courseware.

Lab Setup

Lab A: Using Task Manager and Event Viewer

The lab has no setup requirements that affect replication or customization.

Lab Results

There are no configuration changes on student computers that affect replication or customization.

Overview

Topic Objective
To provide an overview of the module topics and objectives.

Lead-in
In this module, you will learn about optimizing the performance of a computer running Windows XP Professional.

- **Determining System Information**
- **Using Task Manager to Monitor System Performance**
- **Using Performance and Maintenance Tools to Improve Performance**
- **Monitoring Event Logs**

As an Information Technology (IT) professional supporting Microsoft® Windows® XP Professional, you will monitor system resources to evaluate the workload of the computer, observe changes and trends in resource usage, test configuration changes, and diagnose problems. These procedures enable you to optimize the performance of the computer.

Windows XP Professional provides tools for monitoring system resources. System Information presents a comprehensive overview of the hardware, system components, and software environment. Task Manager presents a snapshot of programs and processes that are running on the computer, and provides a summary of the computer's processor and memory usage. Performance and maintenance tools enable you to find and correct system problems such as non-responding programs.

Additionally, the application and system event logs record specific user activities and Windows XP Professional activities, called *events*. Monitoring and analyzing system and application events enables you to identify problems and trends of resource usage, which will help you to improve the performance of the computer.

After completing this module, you will be able to:

- Determine important system information to assist in troubleshooting.
- Monitor computer performance by using Task Manager.
- Improve computer performance by using the tools in Performance and Maintenance in Control Panel.
- Monitor and interpret application and system events.
- Manage event logs.

Determining System Information

Topic Objective
To describe the processes for determining system information.

Lead-in
Before you can optimize the performance of a computer, you need to know specific system information.

- System Summary
- Hardware Resources
- Components
- Software Environment

Windows XP Professional provides an easy way to determine the operating system and BIOS versions running on the computer, and to find information about memory, hardware resources, components, and the software environment. This information is collectively known as *system information*.

To gain access to system information, click **Start**, point to **More Programs**, point to **Accessories**, point to **System Tools**, and then click **System Information**.

System information is organized into the following four top-level categories:

Delivery Tip
Explain that viewing system information is an excellent way to determine if a computer meets upgrade requirements. Also, explain that upgrades often require the latest version of the BIOS, which can usually be downloaded from the manufacturer's Web site.

- System Summary

  The System Summary folder contains the name, version, and other information about the operating system and the basic input/output system (BIOS), and information about the processor and available memory. You can use this information to determine if the computer has the latest BIOS version, or to determine the amount of memory that the computer contains.

- Hardware Resources

  The Hardware Resources folder contains information about resource assignments and possible sharing conflicts among direct memory access (DMA), forced hardware, input/output (I/O), interrupt requests (IRQs) and memory resources. You can use this information to determine which resources, such as ports, that hardware devices are using or sharing, and to resolve resource conflicts.

Delivery Tip
Explain that if they suspect that a hardware problem is related to a driver, they should carefully review the information in this folder.

- Components

  The Components folder contains information about each component in your computer, including the version of the device driver that it is using. The Problem Devices folder under Components is especially useful, as it contains a list of devices for which the driver is currently damaged.

- Software Environment

  The Software Environment folder contains information about the system configuration, including details about system and device drivers, environment variables, and network connections. You can use this information to determine which driver version that a device is using, and which services and tasks are currently running on the computer. Additionally, you can find the name and version of, and path to, dynamic-link libraries (DLLs) associated with any application. The information in this folder is especially useful when a program has difficulty locating a DLL.

Note You can gain access to context-sensitive Help about any folder or subfolder under System Information by right-clicking the folder, and then clicking **What's This?**

When additional applications, such as Microsoft Internet Explorer, are installed, System Information includes application-specific information such as application location and security settings in a dedicated folder.

◆ Using Task Manager to Monitor System Performance

Topic Objective
To identify topics related to monitoring system resources by using Task Manager.

Lead-in
Task Manager provides information about programs and processes running on a computer.

- **Monitoring Applications**
- **Monitoring Processes**
- **Monitoring Performance**
- **Monitoring Network Connectivity**

Ensure that students can define a process.

Task Manager is a tool that provides real-time information about applications currently running on your computer. The available information about applications includes the amount of processor time and memory that the processes associated with the application are using. Task Manager also provides information about the computer's performance and network connectivity.

Important A *process* is a program running in reserved memory space that performs a specific task, such as starting a program. A process, which can run in the foreground or the background, can be part of an application, and an application can have many processes. Winword.exe and Services.exe are examples of processes.

You can use Task Manager to identify an application or process that is using a disproportionate amount of system resources. In addition, the Task Manager status bar provides you with measurements of system or program activity.

To gain access to Task Manager, press CTRL+ALT+DELETE, and then click **Task Manager**.

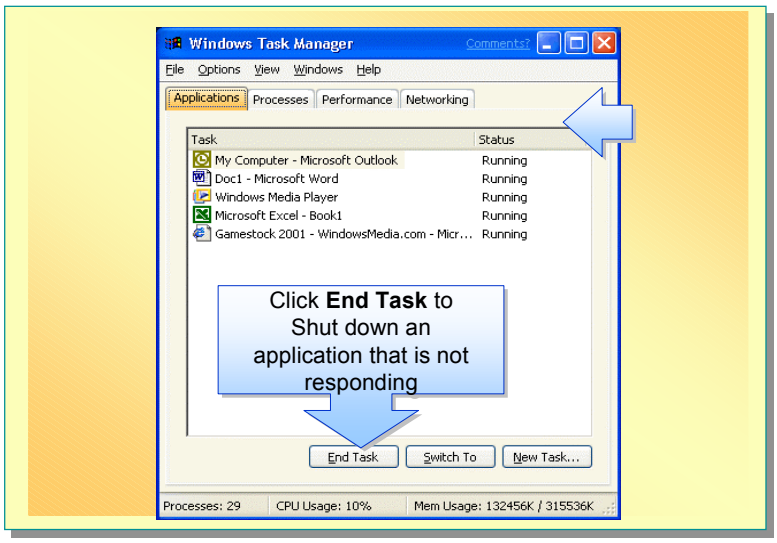
Delivery Tip
Remind students that they configured Ctrl+Alt+Delete options while configuring local security in Module 5, "Configuring Microsoft Windows XP Professional to Operate in a Microsoft Windows Network," in Course 2272A, *Implementing and Supporting Microsoft Windows XP Professional (Course Beta)*.

Note You can restrict access to Task Manager by configuring Ctrl+Alt+Delete options. For more information about configuring Ctrl+Alt+Delete options, see Module 5, "Configuring Microsoft Windows XP Professional to Operate in a Microsoft Windows Network," in Course 2272A, *Implementing and Supporting Microsoft Windows XP Professional (Course Beta)*.

Monitoring Applications

Topic Objective
To illustrate the interface for monitoring applications by using Task Manager.

Lead-in
You use the **Applications** tab to view the status of programs running on a computer.



Explain that the **Application** tab lists only applications that are running in the current user's security context. Ensure that students understand what a security context is.

The **Applications** tab in Task Manager enables you to view the applications currently running in the logged on user's security context. A *security context* is made up of the user's profile and privileges.

Viewing the **Applications** tab should be the first steps in troubleshooting computer performance. For example, if a particular application seems to be functioning slowly, or has stopped functioning, the Applications tab can be viewed to determine the status of the applications. The applications are each listed with a status of **Running** or **Not Responding**.

You can perform the following tasks on the **Applications** tab:

Delivery Tips
Demonstrate ending an application. You will need to have an application running that you can end.

Next, demonstrate identifying the process associated with an application.

- View the status of an application.
- Shut down a non-responding application by selecting the application, and then clicking **End Task**.

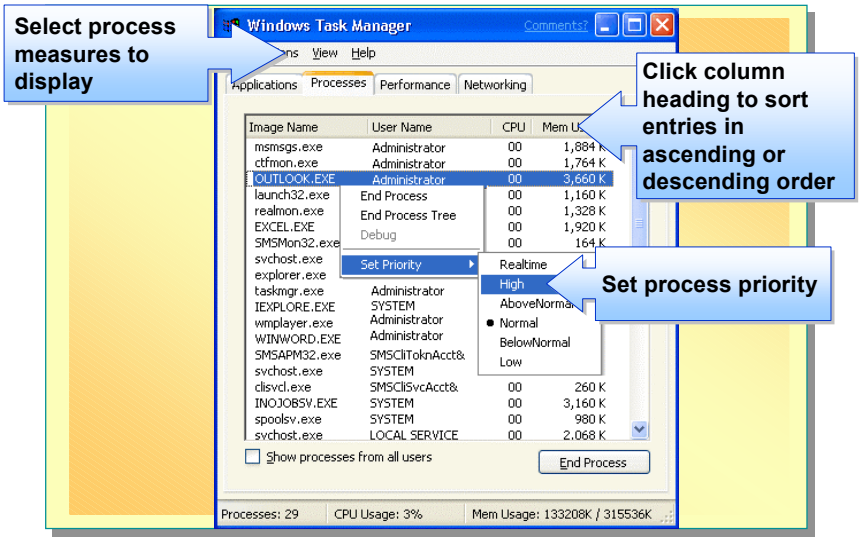
Caution Any data that was entered in the application before it stopped responding will be lost if the data was not saved.

- Switch to another running application by selecting that application, and then clicking **Switch To**.
- Start a new application by clicking **New Task**, and in the **Create New Task** dialog box, typing the exact name of the resource that you want to open. **New Task** is identical to the **Run** command on the **Start** menu.
- Identify the processes that are associated with an application by right-clicking the application, and then clicking **Go To Process**. The **Processes** tab appears and any associated process is highlighted.

Monitoring Processes

Topic Objective
To illustrate the interface for monitoring processes in Task Manager.

Lead-in
You use the **Processes** tab to view information about the processes and programs currently running on your system.



Ensure that students know what an address space is.

Use the **Processes** tab to view a list of running processes and their measures. *Measures* contain information about a process, such as total processor time or the amount of memory the process is using. The list that appears on the **Processes** tab includes all processes that run in their own address space, including all applications and system services. An *address space* is a dedicated portion of memory that is used by the processor.

Both the user and the system can initiate a process, but you can only end a process that is initiated by a user. To end a process initiated by the computer, you may have to restart the computer.

When to View Processes

Each application has at least one associated process, but many have more than one associated process. View the **Processes** tab when you want to determine if a particular process is using a disproportionate amount of memory or CPU time.

You may also need to view the **Processes** tab to end a process. When an application is not responding, closing the application on the **Applications** tab may or may not close all the associated processes. For example, if a mail client is not responding, you can end the application on the **Applications** tab, but you may also need to go to the **Processes** tab and end the SMSAPM32.exe process.

Viewing Process Measures

Explain that 25 process measures are available in Task Manager. The measures shown in the table are the most commonly used.

There are 25 different measures available for each process. You can choose which measures are displayed from the **View** menu. Some of the commonly used process measures available on the **Process** tab in Task Manager are described in the following table.

Property	Description
CPU	The current percentage of the CPU time that is used by the process. If the operating system is not running a specific process, it runs **System Idle Process**, which is a percentage of time that the computer is not processing other tasks. On a system with low utilization, **System Idle Process** may approach 99 percent.
CPU Time	The total processor time, in seconds, used by the process since it was started.
Mem Usage	The amount of main memory, in kilobytes, used by the process.
I/O Read Bytes	The number of bytes read in input/output (I/O) operations generated by a process, including file, network, and device I/Os.
I/O Write Bytes	The number of bytes written in I/O operations generated by a process, including file, network, and device I/Os.
Base Priority	Displays the priority assigned to a particular process. Values are Realtime, High, AboveNormal, Normal, BelowNormal, and Low.

To display other properties, click **View**, and then click **Select Columns**. Select the items that you want to appear as column headings, and then click **OK**.

Using Process Measures to Identify Resource Use

Mention that by sorting the processes, an administrator can determine high-usage processes.

Use the **Process** tab in Task Manager to identify the resource use of a program. Processes can be sorted by any measure, enabling you to view the processes in ascending or descending order for that particular measure.

For example, to identify which process is using the most CPU time, click the **CPU** column. The first time that you click the column it sorts the applications in ascending order of usage. Clicking the column again sorts the applications in descending order of CPU usage. You can only sort by one column at a time.

Promoting and Demoting Process Priority

Each process running on a computer is assigned a base priority. To view the base priority, click **View**, click **Select Columns**, select **Base Priority**, and then click **OK**.

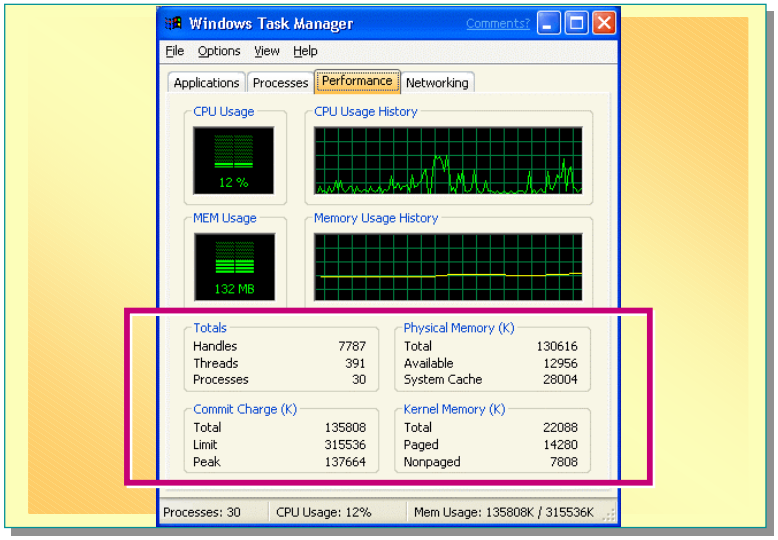
The priority that a process is assigned determines the order in which it can gain access to system resources. Promoting the priority of a process can make it run faster. Demoting the priority of a process can make it run slower. To change the priority assigned to a process, right-click the process, point to **Set Priority**, and then click the priority that you want to assign.

Caution Changing the priority of a process can have adverse effects on that process and other processes. For example, promoting the priority of one process may cause other processes to have less access to the processor, causing them to run more slowly.

Monitoring Performance

Topic Objective
To illustrate the interface for monitoring performance in Task Manager.

Lead-in
The **Performance** tab displays a dynamic overview of your computer's current performance.



To monitor the current performance of your computer, you use the **Performance** tab. While the **Processes** tab shows measures of individual processes, the **Performance** tab shows overall computer performance. This tab displays a dynamic overview of the computer's current performance, including a numeric display and graph of processor and memory usage.

Processes Graphs

CPU Usage displays the current processor usage, and the **CPU Usage History** graph shows the history of processor usage. This history is the combined history of all of the information that you see in the **CPU** column on the **Processes** tab, minus the system idle time.

MEM Usage displays the current memory usage, while the **Memory Usage History** graph shows a combined history of the information in the **MEM Usage** column on the **Processes** tab, minus system idle time.

This table is an overview of the measures on the **Performance** tab. Briefly describe some of the process measures that you can view. Do not go into too much detail, simply select a few to discuss.

Viewing Performance Measures

Some of the performance measures that you can view on the **Performance** tab in Task Manager are described in the following table.

Process measures	Description
Totals	The number of handles, threads, and processes running on the computer. A *handle* is a variable that is used to gain access to a device or object such as a file, window, or dialog box. A *thread* is unit of execution within a process.
Physical Memory	**Total**: Amount of physical RAM, in kilobytes, installed in the computer.
	Available: Amount of physical memory, in kilobytes, available to processes.
	System Cache: Amount of physical memory, in kilobytes, released to the file cache on demand.
Commit Charge	**Total**: Size of virtual memory, in kilobytes, in use by all processes. *Virtual memory* is disk space that is used by the operating system to function as RAM memory.
	Limit: Amount of virtual memory, in kilobytes, that can be committed to all processes without enlarging the paging file. The *paging file* moves pages of data back and forth between physical memory and the hard disk.
	Peak: Maximum amount of virtual memory, in kilobytes, used in the session. If the commit peak exceeds the commit limit, virtual memory is temporarily expanded to accommodate the new peak.
Kernel Memory	**Total**: Sum of paged and nonpaged memory, in kilobytes.
	Paged: Size of the paged memory pool, in kilobytes, allocated to the operating system.
	Nonpaged: Size of the nonpaged memory pool, in kilobytes, allocated to the operating system.

Using Performance Measures to View Processor Time

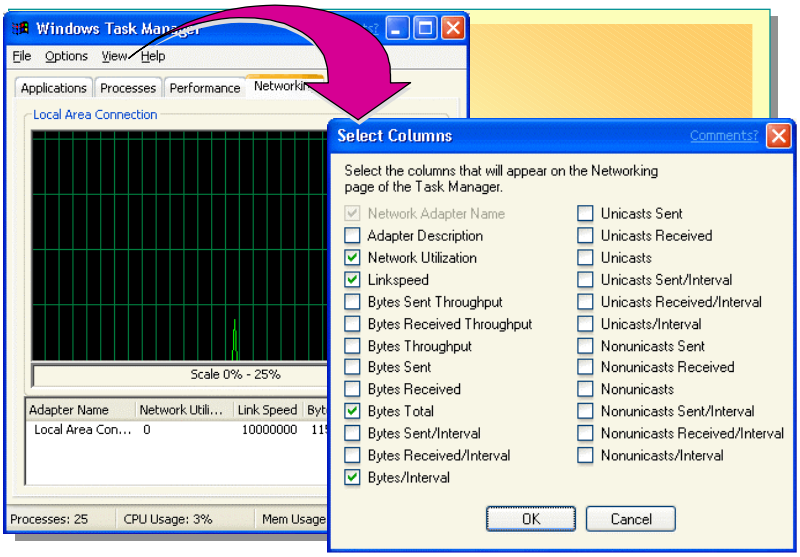
Delivery Tip
Demonstrate how to view processor time in kernel mode.

Use the **Performance** tab in Task Manager to identify the amount of system resources that the operating system or an application is using and to view the percentage of processor time that is being used by the kernel mode. The *kernel* is the core of an operating system that manages memory, files, and peripheral devices, maintains the time and date, launches applications, and allocates system resources.

Monitoring Network Connectivity

Topic Objective
To show the interface for monitoring network connectivity.

Lead-in
You can also use Task Manager to monitor network connectivity.



If you are experiencing problems with a network connection, you can use the **Networking** tab in Task Manager, new in Windows XP Professional, to monitor statistics about network connections currently in use. Monitoring the activity of network connections will enable you to determine if a network connection is functioning properly.

Delivery Tip
If you have more than one network connection, display this tab so that students can see that each connection has its own graph displayed.

The tab, which is available only when network cards are present, has three parts:

- Menus that enable users to configure views and options.
- Charts that show bytes per second through the network interface as a percentage of available bandwidth.

  The bandwidth scale adjusts automatically, and is shown under the graph. There are three possible measures for bytes per second, which are listed in the following table.

Measure (as % of total available bandwidth)	Graph color	Default status
Bytes sent per second	Red	Off
Bytes received per second	Yellow	Off
Total bytes sent/received per second	Green	On

  The graph display can be vertical or horizontal. Configure this option on the **Options** menu. To enable the measure with a default value of Off, on the **View** menu, point to **Network Adapter History**, and then select the measure that you want to view.

- A table that lists measures for each network card.

  The **Adapter Name** column lists the common names of network connections, and the other columns contain measures for each connection. To choose measures, click **View**, click **Select Columns**, and then select the measures that you want to view about each connection.

  Just as you can on the **Processes** tab, you can sort the information by any measure by clicking the column heading for that measure. The first click sorts the information in ascending order, and the second click sorts the information in descending order.

  The following table contains information about the measures on the **Networking** tab that are enabled by default for a LAN connection.

Networking measure	Description
Adapter Name	Name of the adapter as it appears in the Network Connections folder.
Network Utilization	Percent utilization of the network based on the initial connection speed for the interface.
Link Speed	Connection speed of the interface taken from the initial connection speed.
Bytes	The total number of bytes sent and received on the connection to date. The number is cumulative, but can be reset from the Options menu.
Bytes Per Interval	The total number of bytes received on the connection in the in a specific time interval.

  For more information about available network measures, see the Windows XP Professional Help.

Note To conserve memory resources, the **Networking** tab collects data only when Task Manager is open. This function is enabled by the default selection of **Tab Always Active** on the **Options** menu. If you want to collect data only when the **Networking** tab is active, clear the **Tab Always Active** option.

Using Performance and Maintenance Tools to Improve Performance

Topic Objective
To introduce the common performance and maintenance tools and their functions.

Lead-in
Several performance and maintenance tools enable you to easily improve computer performance.

- **Using Maintenance Tools to Improve Performance**
- **Configuring visual Effects for Best Performance**
- **Configuring Processor Scheduling, Memory Usage, and Virtual Memory**

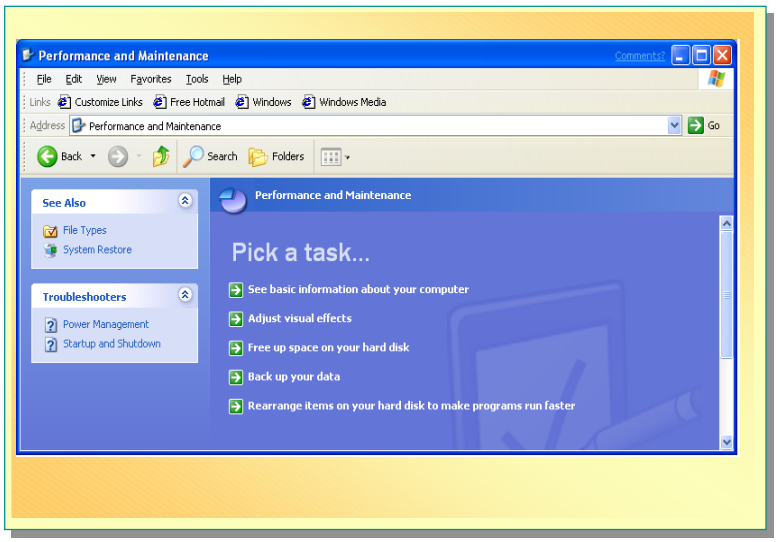
Windows XP Professional provides performance and maintenance tools that enable you to improve the performance of the computer. To gain access to these tools, click **Start**, click **Control Panel**, and then click **Performance and Maintenance**.

Delivery Tip
Demonstrate how to gain access to performance and maintenance tools. Do not present information on these tools now. Do so on the following pages.

Using Maintenance Tools to Improve Performance

Topic Objective
To explain the functions of the maintenance tools.

Lead-in
All of the tools under **Performance and Maintenance**, except **Change settings that affect my computer's performance**, are maintenance tools.



Delivery Tip
Demonstrate these tools.

Key Points
Regularly performing maintenance can help improve the performance of your computer.

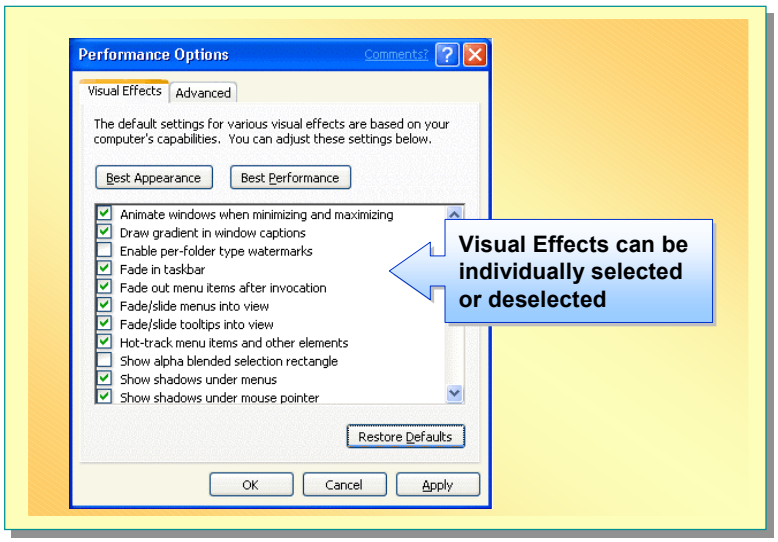
It is important to perform regular maintenance on the computer to improve performance. The following table includes the performance tools found in Control Panel.

Tool	Use to
Adjust Visual Effects	Configure visual effects for the computer, and to configure processor scheduling, memory usage, and virtual memory.
Free up space on your hard drive	Clean up your hard disk by reclaiming space used by temporary files and unnecessary program files.
Rearrange items on your hard disk to make programs run faster	Run the Disk Defragmenter tool to rearrange files, programs, and unused disk space into contiguous segments, resulting in files and programs opening faster.

Configuring Visual Effects for Best Performance

Topic Objective
To describe the options on the **Visual Effects** tab and their affect on computer performance.

Lead-in
The **Change settings that affect my computer's performance** option enables you to configure the visual effects that the computer will use.



When you choose the **Adjust Visual Effects** option, the **Performance Options** property sheet is displayed. The sheet contains two tabs, **Visual Effects** and **Advanced**.

Configuring Visual Effects

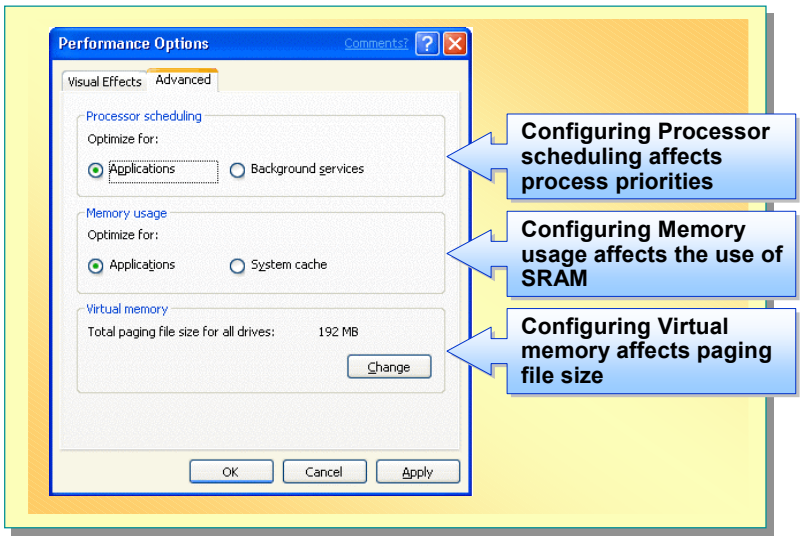
The **Visual Effects** tab enables you to configure visual effects that balance your needs for visual appeal and computer performance. The default settings for the configurable visual effects are based upon your computer's capabilities. You can enable an individual visual effect by selecting its check box, or disable it by clearing the check box. Additionally, you can use three buttons that will automatically configure all of the effects. The buttons and their functions are explained in the following table.

Button	Effect
Best Appearance	Enables all of the available visual effects. This option improves the visual appeal of Windows XP Professional, but may decrease performance by using more memory for visual effects.
Best Performance	Disables all of the available visual effects. This option improves performance by reallocating the memory that the visual effects would have used.
Restore Defaults	Restores the default visual effects settings, which are based on your computer's capabilities.

Configuring Processor Scheduling, Memory Usage, and Virtual Memory

Topic Objective
To describe the processes for and repercussions of configuring Advanced Performance Options.

Lead-in
You can configure processor scheduling, memory usage, and virtual memory on the **Advanced** tab.



The **Advanced** tab of the **Performance Options** property sheet enables you to configure **Processor scheduling**, **Memory usage**, and **Virtual memory**.

Configuring Processor Scheduling

You can optimize Processor scheduling for either **Applications** or **Background services**. These options are described in the following table.

Optimized for	Effect	Use when
Applications	More processor resources are allocated to the foreground program than to any programs running in the background. The priority of the foreground application's process(es) is promoted.	You need the foreground program to run as smoothly and quickly as possible.
Background services	All running programs receive equal amounts of processor resources.	You need to enable background operations, such as a disk backup, to run as quickly as possible.

Configuring Memory Usage

Memory usage can be optimized for either **Applications** or **System cache**. Windows XP Professional caches information on the hard disk for easy retrieval. To do so, the operating system uses a portion of the computer's RAM. When you choose from the configuration options listed in the following table, you are specifying whether the operating system uses more or less RAM for caching.

Optimized for	Effect	Use when
Applications	Applications are given priority use of the computer's RAM. Applications will run faster.	This is the default setting. Always use this setting unless you need to configure for system caching.
System Caching	The operating system is given more RAM to use for swapping paging files, which enables information to be moved from the hard disk to RAM.	Many applications need to run concurrently, causing paging files to be used more frequently.

Configuring Virtual Memory

Virtual memory, or paging file size, can be increased or decreased to affect performance. You should usually not set a paging file to less than the recommended level, which is 1.5 times the amount of RAM in the computer. To configure virtual memory, on the **Performance Options** property sheet, click **Change**, and the **Virtual Memory** property sheet will display.

Paging file size is configured for each drive on each hard disk in the computer. To configure the paging file size, on the **Virtual Memory** property sheet, select the drive, and then choose from the following options.

Option	Use when
Custom size	You want to specify the size of a paging file, especially if you want to increase it over the default size.
System managed size	You want to enable Windows XP Professional to specify the size of the file.
No paging file	You do not want a paging file on the selected drive.

The placement of the paging file in relation to the operating system affects computer performance. A single paging file can be used by all of the partitions in a computer. For best performance on a computer that has multiple hard disks, place the paging file on a disk that does not contain the operating system. For best performance on a computer that has a single hard disk, the paging file should be on the same partition as the operating system.

Important When the paging file does not reside on the same physical disk as the operating system, system failure information cannot be written to the paging file, and thus cannot be reviewed to determine the cause of a system failure.

◆ Monitoring Event Logs

Topic Objective
To identify the topics related to monitoring event logs.

Lead-in
You can monitor a variety of activities and events in Windows XP Professional.

- **Introduction to Event Logs**
- **Types of System and Application Events**
- **Viewing Event Logs**
- **Limiting the Size of Log Files**
- **Archiving Event Logs**

Events are user activities, significant activities in Windows XP Professional, or application activities. Monitoring system and application events enables you to identify and track resource use, system errors, and application errors.

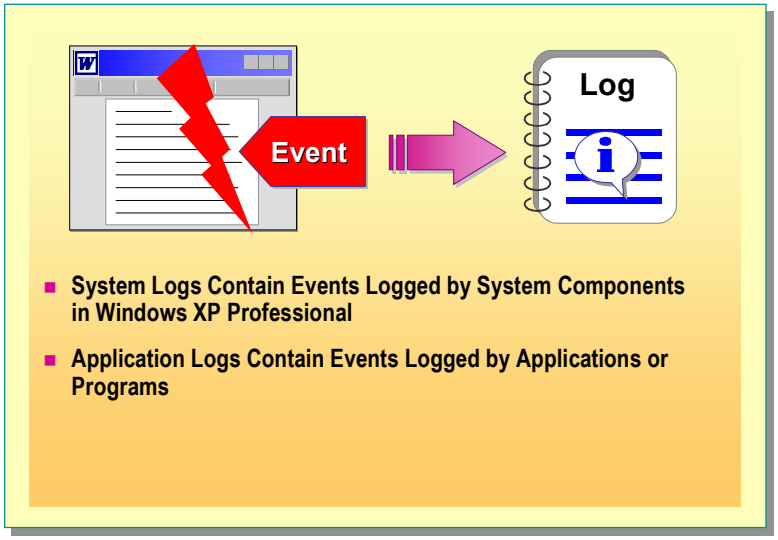
System events, which are automatically configured by Windows XP Professional, are recorded in the System log. *Application events*, which are determined by the application developer, are recorded in the Application log. After events are recorded in these logs, you can view and analyze the logs to detect activities and events that require administrative consideration. Based on your analysis of the logs, you may need address system problems or reallocate resources. You may also need to address changes in application configuration or system configuration.

Note Security events, based on an audit policy, are recorded in the Security log. For more information about the Security log and audit policies, see Module 9, "Monitoring Event Logs" in Course 2028A, *Basic Administration of Microsoft Windows 2000.*

Introduction to Event Logs

Topic Objective
To illustrate an example of the actions associated with events and event logs.

Lead-in
Event logs enable you to monitor information about hardware, software, and system problems.



Event logs enable you to monitor information about hardware, software, system problems, and security. You view these logs to detect activities and events that require your attention. Logs can also be used to provide a history of events. You use Event Viewer to view event logs.

To open Event Viewer, click **Start**, click **Control Panel**, click **Performance and Maintenance**, click **Administrative Tools**, and then double-click **Event Viewer**.

Windows XP Professional records events in three logs:

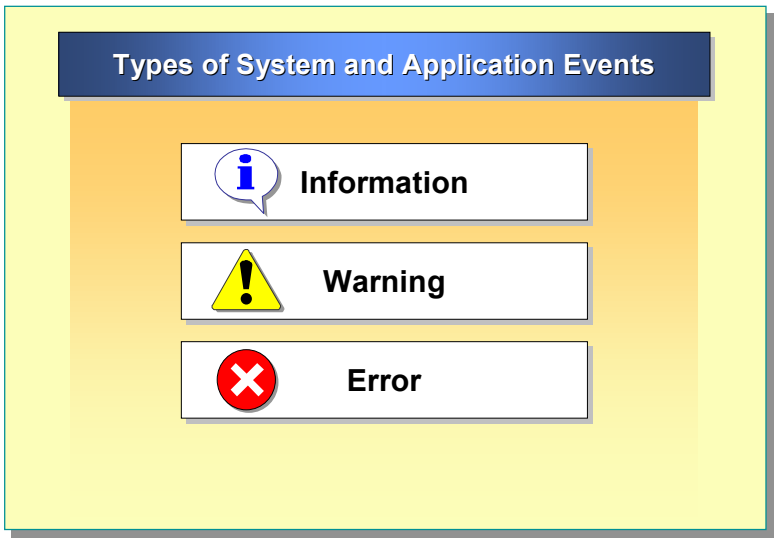
- *System log*. This log contains events generated by the system components in Windows XP Professional. For example, if a driver or other system component fails to load during startup, this failure is recorded in the system log. Windows XP Professional predetermines the event types logged by system components.
- *Application log*. This log contains events generated by applications. For example, a database program would record a file error in the Application log. The program developer decides which events to record. Dr. Watson application logs are also viewable in this log. Dr. Watson for Windows XP Professional is a program error debugger. When an application exception, or program error, occurs, Dr. Watson generates a log file called Drwtsn32.log.
- *Security log*. This log records security events, such as valid and invalid logon attempts, and events related to resource use, such as creating, opening, or deleting files. An administrator specifies what events are recorded in the Security log. For example, if you have enabled logon auditing, all attempts to log on to the system are recorded in the security log.

Note All users can view application and system logs, but security logs are accessible only to system administrators.

Types of System and Application Events

Topic Objective
To illustrate the types of system and application events.

Lead-in
There are three types of system and application events: information, warnings, and errors.



System and application developers determine the system and application events that are recorded. Each event contains detailed information, such as the type of event and the service associated with the event. The three types of system and application events, Information, Warning, and Error, are described in the following table.

Delivery Tip
Demonstrate opening the System log, and explain a few of the events recorded there.

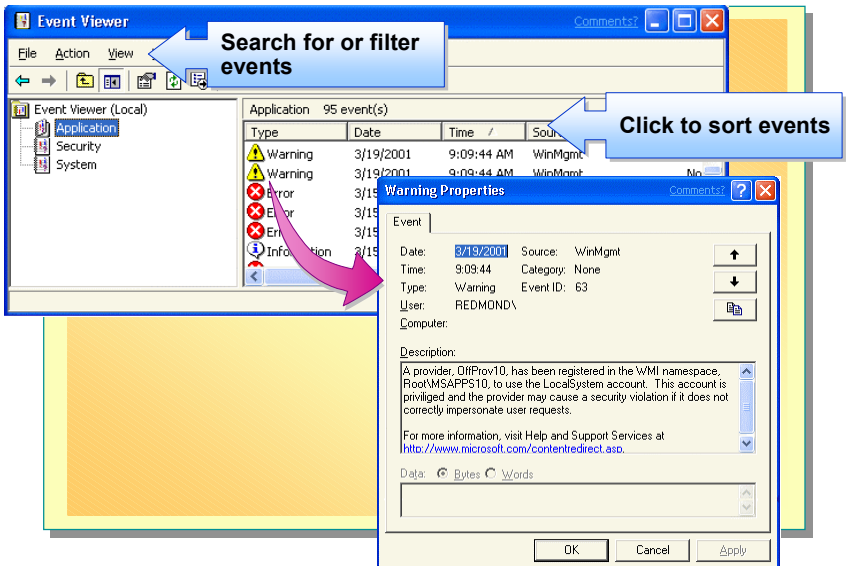
Type of event	Description
Information	The successful operation of an application, driver, or service. For example, when a significant service, such as the Event Log service, starts successfully, Windows XP Professional will log an Information event.
Warning	An event that is not necessarily urgent, but may indicate a future problem with system operations. For example, when disk space is low, Windows XP Professional will log a warning. A virus detection program may log an error when a virus is detected.
Error	A significant problem with system operations, such as loss of data or loss of functionality. For example, if a service fails to load during startup, Windows XP Professional will log an error.

Note Security events have additional event types. For more information, see Module 9, "Monitoring Event Logs," in Course 2028A, *Basic Administration of Microsoft Windows 2000.*

Viewing Event Logs

Topic Objective
To illustrate the interface for viewing event logs.

Lead-in
Use Event Viewer to view the event logs, which you can use to monitor information about hardware, software, and system problems.



System and application events are by default sequentially logged in their associated log files, from most recent to oldest. The log files contain information about each event that occurs. You can monitor information about hardware, software, and system problems by viewing the System and Application event logs in Event Viewer.

Delivery Tip
Demonstrate Event Viewer. Select a log to view and point out the event properties in the log.

Use Event Viewer to view detailed information about each event in a log. Select the log that you want to view in the console tree of Event Viewer. In the details pane, Event Viewer displays a list of log entries and summary information for each entry.

Note In addition to viewing a log locally, you can also view a log for a remote computer. To view a log on a remote computer, in Event Viewer, right-click **Event Viewer (Local)** and then click **Connect to another computer**. In the **Select Computer** dialog box, verify that **Another computer** is selected, and then type the name of the computer.

Delivery Tip
Demonstrate the three methods for locating events. Discuss some of the properties listed in the tables.

Locating Events

To facilitate your analysis of events, you can search for specific events, filter the events included in the details pane, or sort the events by a particular measure. Each method is described as follows:

- Search for specific events by using the **Find** command on the **View** menu. For example, if a particular event seems related to system problems, search the System log to find other instances of the same event to assess the frequency of an error.
- Search for a group of events by filtering the log. To filter the log, click **View**, click **Filter**, and then select filter criteria. For example, if you suspect that a hardware component is the origin of system problems, filter the System log to show only the events generated by that component.

  The event properties that you can use to filter out specific events are described in the following table.

Property	Description
Event types	The type of event to view.
Event source	The application or component driver that logged the event.
Category	The category of event, such as a logon or logoff attempt.
Event ID	An event number used to identify the event. This number helps product support representatives to track events.
User	A user logon name.
Computer	A computer name.
From: **To:**	The range of events to view from first date to last date to last.

- Sort the events in the log by clicking on the heading of a particular data column. The first click sorts the data in ascending order, and the second click sorts the data in descending order. For example, you can click **Source** to sort the events in a log by the source of the event.

Examining Event Properties

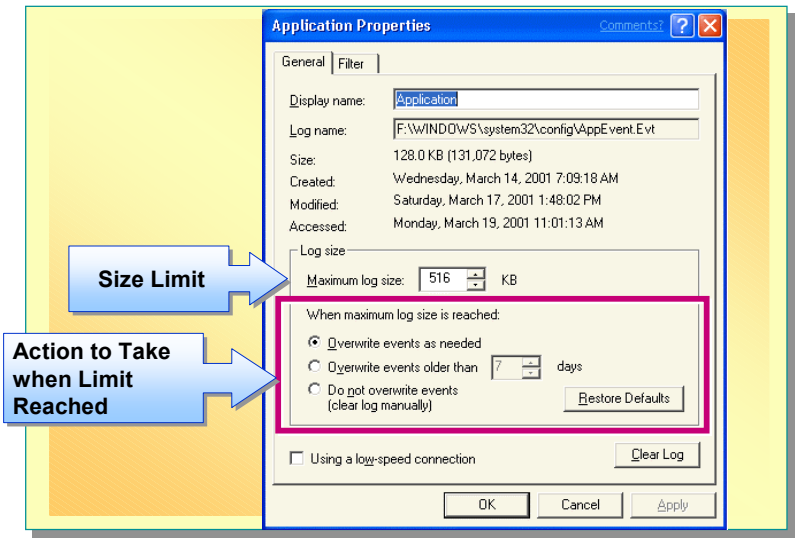
In addition to the date, time, and event ID, you can view the event properties that are described in the following table. View event properties by double-clicking the event.

Property	Description
Source	Displays the system component, application, or security event in Windows XP Professional that generated the log.
Category	Defines the event, as set by the source, so that the programmer can further define the event as it occurs.
Type	Displays the type of event: Error, Warning, or Information.
User	Displays the user name if the event is attributed to a specific user.
Computer	Displays the exact name of the computer where the logged event occurred.
Description	Displays a text description of the event. Text descriptions are created by the source of the event.
Data	Displays binary data generated by the event. Someone familiar with the source application can best interpret this information.

Limiting the Size of Log Files

Topic Objective
To illustrate the interface for limiting the size of event log files.

Lead-in
You can control the size of the logs and specify the action to take when a log becomes full.



Key Points
If you are tracking trends over time, you will want to archive old event entries instead of overwriting them.

You can limit the size of event logs if hard disk space is a concern. If you limit the log size, you must select a method to overwrite older log event entries with new log entries.

Note If your security needs are high or you want to keep a history of events, you can choose to archive old event entries instead of overwriting them.

To configure the size of logs, select the log in Event Viewer, and then display the **Properties** dialog box for the log. In the **Properties** dialog box for each event log, you can configure:

- The size of the log, which can range from 64 kilobytes (KB) to 4 gigabytes (GB). The default size is 512 KB.
- The action that Windows XP Professional takes when a log is full. You can choose from the options described in the following table.

Option	Description
Overwrite events as needed	You may lose information if the log becomes full before you archive it. However, the setting requires no maintenance. Choose this option when you review the log frequently, so that you will review events before they are overwritten. You should not use this option when security is a priority.
Overwrite events older than *x* days	Enter the number of days. You may lose information if the log becomes full before you review or archive it, but you will only lose information older than the days that you specified. Choose this option when you review the log every three to five days.
Do not overwrite events (clear log manually)	This option requires you to clear the log manually. When a log becomes full, Windows XP Professional will stop recording events in the log. However, Windows XP Professional does not overwrite any security log entries. Choose this option when security is a high priority, and you do not want to lose any logged events.

Manually Clearing an Event Log

If you click the **Do not overwrite events (clear log manually)** option, you must periodically archive and clear the log manually. When the log is full, Windows XP Professional displays a status message indicating that the log is full. In addition, Windows XP Professional can be configured to shut down when the security log is full. Shutting down prevents someone from overwriting the security logs to hide activities that may compromise the security of your network. It is also important to configure a log file size that is large enough to accommodate the log files until they are archived and cleared.

Delivery Tip
Open the interface and show the students where to manually clear an event log, but *do not* clear the log.

To clear an event log, perform the following steps:

1. In the console tree, click the log you want to clear.
2. On the **Action** menu, click **Clear all Events**.
3. Click **Yes** to save the log before clearing it.

   –or–

   Click **No** to permanently discard the current event records and start recording new events.

Archiving Event Logs

Topic Objective
To identify the purpose and procedure for archiving event logs.

Lead-in
You archive logs to maintain a history of logged events and compare logs from different times to track trends.

- **Archive Event Logs To:**
  - Track trends to determine resource usage
  - Track use of resources
  - Keep records when required by law
- **Select a File format to View Archived Logs in Other Applications**
  - Log-file format (.evt)
  - Text-file format (.txt)
  - Comma-delimited text-file format (.csv)

You archive event logs to make them accessible for later retrieval and analysis. When archiving event logs, you can determine the format that they are saved in.

Reasons for Archiving Event Logs

Delivery Tip
Demonstrate how to archive a log, view a log, and clear an archived log.

You archive logs to maintain a history of logged events and compare logs from different times to track trends. Viewing trends can help you determine if a particular application or system problem is occurring consistently or with increasing frequency. Many organizations have policies for saving archived logs for a specified period of time. Some organizations, such as government agencies and banks, are required by law to save archived logs.

Mention the options that are available when archiving a log.

To archive a log or to view an archived log, select the log in Event Viewer. On the **Action** menu, click one of the options described in the following table.

To	Do this
Archive the log	Click **Save Log File As**, and then type a file name.
View an archived log	Point to **New**, and then click **Log View**. In the **Add Another Log View** dialog box, click **Saved**, and then provide the path to the log.

Selecting a File Format

You can save event logs in different formats so that you can view log data in other applications. For example, use a spreadsheet application, such as Microsoft Excel, to manipulate data so that you can more easily track trends. You can save event logs in one of three file formats:

- Log-file format (.evt). Enables you to view the archived log again in Event Viewer.
- Text-file format (.txt). Enables you to view the information in a word processing program such as Microsoft Word.
- Comma-delimited text-file format (.csv). Enables you to view the information in a spreadsheet or database program, such as Excel..

Key Point
The text-file or comma-delimited text-file format of an event log does not contain the binary data normally contained in an event. This means some information is lost when saving a log in either of these formats.

Important Logs saved in text-file or comma-delimited text-file format do not retain the binary data contained within the event. This binary data may contain additional information to aid you in troubleshooting.

Lab 14A: Using Task Manager and Event Viewer

Topic Objective
To introduce the lab.

Lead-in
In this lab, you will monitor applications and events to determine the source of computer problems.

Objectives

After completing this lab, you will be able to:

- Monitor application performance by using Task Manager.
- Shut down applications by using Task Manager.
- Review computer activity by using Event Viewer.
- Manage event logs.
- Find information in event logs.

Lab Setup

To complete this lab, you need the following:

- Completed Lab 1C Upgrading Windows 98 to Windows XP Professional.
- A computer running Windows XP Professional.
- Lab files are located on the Student CD in the Labfiles folder. The required files are: App1-1.exe, App1-2.exe, App1-3.exe, App1-4.exe, App1-5.exe, Lab12.cmd, and Syslog.csv.

Estimated time to complete this lab: 45 minutes

Review

Topic Objective
To reinforce module objectives by reviewing key points.

Lead-in
The review questions cover some of the key concepts taught in the module.

- Determining System Information
- Using Task Manager to Monitor System Performance
- Using Performance and Maintenance Tools to Improve Performance
- Monitoring Event Logs

1. You are experiencing problems with a hardware component. You are unsure if the problem is related to the device driver, or the port that the device is using. Describe how to easily find information on the device driver and the port.

   You can use System Information to find this information. The Hardware Resources folder will provide information on the port, including conflicts and sharing. The Components folder will provide information on the version of the driver. The Problem Devices folder within Components is a good place to begin researching a problem device.

2. You are running three memory-intensive applications on a computer. You want to ensure that a given application always has the processor time that it needs. How can you accomplish this?

   On the Application tab of Task Manager, find the process(es) associated with the given application. On the Process tab, promote the priority of the process(es) to High or Realtime.

3. A user calls and complains that his network connection doesn't seem to be sending or receiving information efficiently. How can you find information on the speed of the information being sent and received?

   On the Networking tab of Task Manager, enable the graph for that network connection to show bytes sent per second, bytes received per second, and total bytes per second. These bytes are shown as a percentage of bandwidth, enabling you to determine how much of the available bandwidth of the network connection is being used.

4. A user complains that her applications all seem to be running more slowly than usual. What maintenance options may help solve this problem?

   The Free up space on my hard drive and Rearrange items on my hard disk to make programs run faster.

5. You want to run virus-scanning software on a computer. It runs in the background, and you want to run it as quickly as possible. What configuration settings could you change to ensure that while running in the background the application receives the resources it needs?

   On the Advanced tab of the Performance Options property sheet, choose to optimize processor scheduling for background operations.

6. You suspect that a particular application is causing a degradation of performance on a computer. Describe ways to locate related events in the Application log.

   Search for events generated by the suspect application by using the Find command on the View menu.

   Filter the log by event type and by event source so that only errors and warnings generated by the suspect application are shown.

   Sort the log by event source, and then examine all the events related to the suspect application. You could also sort by any other measure.