

Chapter 15

Windows Operating Systems

At a Glance

Instructor's Manual Table of Contents

- Overview
- Objectives
- Teaching Tips
- Quick Quizzes
- Class Discussion Topics
- Additional Projects
- Additional Resources
- Key Terms

Lecture Notes

Overview

The products now categorized as Windows operating systems are descended from a series of graphical interfaces designed to work with or “on top of” Microsoft’s MS-DOS operating system. Over time, Windows evolved into complex operating systems independent of MS-DOS.

This chapter discusses Windows operating systems in general, though it provides greater coverage of the operating systems built on the Windows NT kernel, including Windows XP Professional and Windows Server. It begins by presenting the development of the Windows operating system and the design goals. The role of the Memory Manager, especially the Virtual Memory Manager, is discussed. The use of the Device, Processor, and Network Managers in recent versions of Windows is reviewed. The chapter then explains the role of the file system in file management and the challenges for Windows system security today. The chapter concludes by explaining how the current Windows user interface functions. Throughout this chapter, many acronyms are introduced to describe this networked operating system. A list of the Microsoft acronyms can be found in Appendix B.

Learning Objectives

After completing this chapter, the student should be able to describe:

- The role of MS-DOS in early Windows releases
- The design goals for Windows operating systems
- The role of the Memory Manager and Virtual Memory Manager
- The use of the Device, Processor, and Network Managers in recent versions of Windows
- The challenges for Windows system security
- How the current Windows user interface functions

Teaching Tips

Windows Development

1. Provide students with a brief overview of Windows development, noting that the first Windows product used a graphical user interface (GUI) as its primary method of communication with the user.
2. Remind students that a comparison of GUIs from several operating systems is available in Appendix C.

Early Windows Products

1. Provide students with a brief overview of Windows development, using Table 15.1 on page 460 as a guide.
2. Provide students with a brief introduction to Windows for Workgroups, which was the first Windows product to accommodate the needs of network users by including programs and features for small LANs.

Operating Systems for Home and Professional Users

1. List the disadvantages of running early Windows operating systems on top of MS-DOS, such as little built-in security, no multitasking capability, no interprocess communication capability, and the difficulty in moving the OS to other platforms.
2. Discuss Microsoft's response to these disadvantages.
3. Provide students with an overview of the evolution of key Microsoft Windows operating systems for home and professional use, using Table 15.2 on page 461 as a guide.

Operating Systems for Networks

1. Provide students with an overview of the development of more powerful networking products, beginning with Windows NT ("New Technology"). List the primary market requirements that were identified for Windows NT. Point out that unlike the single-user versions of Windows, Windows NT never relied on MS-DOS for support.
2. Explain the evolution of key Microsoft Windows networking operating systems, using Table 15.3 as a guide. Mention that all Microsoft networking operating systems have evolved from Windows NT.
3. List different versions of Windows NT and Windows 2000 and explain their key features.
4. Discuss the advantages that the Server and Advanced Server editions of Windows introduced.

Teaching Tip	Refer to the following Web site to learn more about the history of Windows operating systems: www.microsoft.com/windows/WinHistoryIntro.mspx
---------------------	--

Design Goals

1. Explain why the designers of the Windows operating system had to incorporate a set of software design goals to facilitate decision making as the coding process evolved.

2. Explain that when they were designed, Windows networking operating systems were influenced by several operating system models and incorporated already existing frameworks while introducing new features. Discuss the object model.
3. List the five design goals that the Windows design team identified to accommodate the various needs of its users and to optimize resources: extensibility, portability, reliability, compatibility, and performance.

Extensibility

1. Discuss the concept of extensibility, which refers to the ability of the system to be easily enhanced.
2. Discuss the separation of Windows functions into a privileged executive process and the set of nonprivileged processes called “protected subsystems.” Explain how these help to ensure the integrity of the Windows operating system.
3. Briefly explain four more features that were included to ensure integrity: modular structure, objects, the capability of adding drivers at any time, and remote process calls.

Portability

1. Explain the concept of portability, the operating system’s ability to operate on different machines based on different processors or configurations. List the guidelines that the Windows development group followed to achieve this goal.
2. Discuss briefly the key portability features of Windows NT and its successor systems, such as the use of modular code, the fact that the OS was written in C, and the hardware extraction layer (HAL).

Reliability

1. Discuss the concept of reliability, which refers to the robustness of a system and its ability to protect itself and its users from accidental or deliberate damage by user programs. Briefly explain the different features that strengthen Windows systems.

Compatibility

1. Explain the concept of compatibility, which refers to an operating system’s ability to execute programs written for other operating systems or for earlier versions of the same system. Explain how this feature is addressed in Windows operating systems.

Performance

1. Discuss the features that help Windows achieve good performance levels, i.e., fast and efficient performance. Use the bullet points on page 466 as a guide.

**Teaching
Tip**

Demonstrate performance and reliability in a Windows system by pressing the Windows logo key and the R key together. Then type perfmon.msc. Click OK to see the performance monitor.

Quick Quiz 1

1. Which of the following Microsoft Windows networking operating systems includes a Web edition?

- a. Window NT 4.0
- b. Windows 2000
- c. Windows Server 2003
- d. All of the above

Answer: c

2. Which of the following is a design goal of the Windows operating systems? (Choose all that apply.)

- a. Extensibility
- b. Profitability
- c. Compatibility
- d. Performance

Answer: a, c, and d

3. Which of the following file systems is supported by recent versions of Windows operating systems? (Choose all that apply.)

- a. POSIX
- b. CDFS
- c. NTSC
- d. NTFS

Answer: b and d

Memory Management

1. Provide students with an overview of memory management in Windows operating systems. Discuss the concept of virtual memory.
2. Point out the challenges involved in memory management for all Windows operating systems, e.g., the challenge of running application programs written for Windows, MS-DOS, or POSIX without programs crashing into each other's memory.
3. Discuss the layout of memory in recent versions of Windows, using Figure 15.1 on page 467 in the text as a guide.

User-Mode Features

1. Discuss briefly the Virtual Memory (VM) Manager and the services that it provides, using the bullet points on pages 467-468 in the text as a guide.

Virtual Memory Implementation

1. List the two techniques on which the Virtual Memory Manager relies, namely address space management and paging.
2. Provide students with a brief overview of address space management, using Figure 15.1 on page 467 as a guide. Point out that the upper half of the virtual address space is accessible only to kernel-mode processes, and that code in the lower part of this section, kernel code and data, is never paged out of memory.
3. Discuss the function of the pager. Point out that it is a complex combination of software policies and hardware mechanisms. Briefly discuss these software policies and hardware mechanisms, including their roles.
4. Explain the paging policies, including the fetch, placement, and replacement policies.

Teaching Tip	Refer to the following Web site to learn more about memory management in Windows operating systems: http://msdn2.microsoft.com/en-us/library/aa366779.aspx
---------------------	--

Processor Management

1. Provide students with an overview of processor management in Windows operating systems. Stress that Windows is a preemptive-multitasking, multithreaded operating system.
2. Remind students of the concepts of threads, including their contents (the thread's context) and their purpose.
3. Explain unitasking and multitasking in Windows, using Figures 15.2 and 15.3 on page 471 in the text as a guide. Point out that in multitasking, all threads belonging to one process share its global variables, heap, and environment strings.
4. Discuss the advantages of multithreading.

Device Management

1. Provide students with an overview of device management in Windows operating systems.

2. List the different features that the I/O system in Windows NT and its networking descendents provided, using the bullet points on page 472 as a guide.
3. Describe the packet-driven I/O system in Windows operating systems. Discuss the roles of the I/O Manager and the driver in creating and receiving an I/O request packet (IRP).
4. Discuss the additional tasks of the I/O manager.
5. Discuss the need for a device-independent model for I/O services and the concept of a “multilayered device driver” in Windows operating systems. Explain the importance of a “multilayered device driver.” List the routines of a device driver.
6. Discuss the concepts of driver object and device object that are useful in determining which driver should be called to process the request. Explain how an application instruction results in disk access, using the examples shown in Table 15.4 and Figure 15.4 on page 474 as a guide.
7. Discuss the advantages of representing devices and drivers with different objects.
8. Explain how the I/O Manager interacts with a layered device driver to satisfy a user command, using the example shown in Figure 15.5 on page 475.
9. Mention that the I/O Manager knows nothing about the file system. Outline the differences between a single-layer and a multilayer device driver approach. Provide examples of devices for which such approaches are used. Be sure to mention that there is overhead involved when the I/O Manager passes requests for information back and forth.
10. Explain the asynchronous I/O operation feature that is unique to current Windows operating systems.

Teaching Tip	Refer to the following Web site to learn more about device management technologies: http://technet2.microsoft.com/windowsserver/en/library/adfc5b1c-4105-47a6-8388-de92891e8d0a1033.mspx?mfr=true
---------------------	--

File Management

1. Provide students with an overview of important features of file management in Windows operating systems. Point out that current versions of Windows are designed to be independent of the file system on which they operate. List the different file systems for hard disks supported by Windows.
2. Explain the concepts of virtual file, file handles, and file objects in file management.

3. Use Figure 15.6 on page 478 to illustrate the contents of file objects and the services that operate on them. Use Table 15.5 on page 478 in the text to illustrate the object body attributes.
4. Discuss the distinction between a file object, a memory-based representation of a shareable resource that contains only data unique to an object handle, and the file itself, which contains the data to be shared.
5. Using an example such as the one provided on page 479 in the text, explain the concept of “mapped file I/O,” which is an important feature of the I/O system and is achieved through the cooperation of the I/O system and the VM Manager.
6. Point out that the file management system supports long filenames that can include spaces and special characters. Moreover, the file management system can automatically shorten filenames when required.

Network Management

1. Provide students with an overview of network management in Windows operating systems. Point out that networking is an integral part of the Windows NT-based operating systems. List the services that networking provides.
2. Explain the concept of named pipes to provide a high-level interface for passing data between two processes regardless of their locations.
3. Explain the concept of Mailslots to provide one-to-many and many-to-one communication mechanisms useful for broadcasting messages to any number of processes.

MS-NET

1. Provide students with an overview of Microsoft Networks (MS-NET), which became the model for the NT Network Manager.
2. Explain the three MS-NET components: the redirector, the server message block (SMB) protocol, and the network server. Discuss their key features and functions.
3. Explain how the seven layers of the OSI reference model are implemented in current Windows network management, using Figure 15.7 on page 481 as a guide.

Directory Services

1. Explain the concept of Active Directory, which is a general-purpose directory service for a heterogeneous network. Discuss its key features. Make sure students understand DNS and LDAP.
2. Describe how Active Directory clients locate objects on the network using standard DNS and LDAP protocols. Use Figure 15.8 on page 482 as a guide.

Teaching Tip	Refer to the following Web site to learn more about network management in Windows operating systems: http://msdn2.microsoft.com/en-us/library/aa370672.aspx
---------------------	---

Teaching Tip	Refer to the following Web site to learn more about active directory in Windows 2003 server: http://support.microsoft.com/kb/818626
---------------------	--

Security Management

1. Briefly discuss the object-based security model that Windows network operating systems provide. Point out that one of the biggest concerns in Windows operating systems is the need for aggressive patch management to combat many viruses and worms that target these systems.

Security Basics

1. Discuss the features that Windows operating systems include to comply with the Class C2 level of security, using the bullet points on page 483 as a guide.
2. Discuss the multilayered security system that Windows uses to prevent access by unauthorized users while allowing entry to legitimate users.

Security Terminology

1. Discuss the built-in security feature of recent Windows network operating systems, which is a necessary element for managers of Web servers and networks.
2. Describe how security is implemented using Kerberos.
3. Explain that every user who wants to securely access remote services must log on to a Kerberos server. Use Figure 15.9 on page 484 in the text to illustrate the path followed by a request from an application to a service provided on the network.

Teaching Tip	Refer to the following Web site to learn more about Microsoft Kerberos: http://msdn2.microsoft.com/en-us/library/aa378747.aspx
---------------------	--

User Interface

1. Provide students with an overview of the user interface in Windows operating systems. Point out the options to start or to quit an application in Windows operating systems.
2. Briefly discuss the Start Menu, which organizes files and programs into logical groups. Outline different functions that users can perform from the Start Menu. Use Figure 15.10 on page 484 to illustrate a typical Start Menu.
3. Discuss how the Start Menu organizes files and programs into logical groups and the common functions of the Start Menu.
4. Discuss the utility of the Windows Task Manager and Windows Explorer. Use Figures 15.11 and 15.12 on pages 486 and 487 to illustrate these features.
5. Discuss security in Windows networked systems. Note the tools to help users identify and access network resources (folders, printers, and connections to other nodes). Explain and demonstrate them by:
 - a. Going to the Network and Sharing Center
 - b. Clicking on View Computers and Devices
 - c. Clicking the option to map a network drive

Illustrate these steps pictorially using Figure 15.13 on page 488 in the text.

6. Briefly discuss various other features including the command interface, keyboard shortcuts, the onscreen keyboard, built-in input methods, fonts for many languages, and the resource monitor.
7. Illustrate these features pictorially using Figures 15.14 through 15.17.

Teaching Tip	For a list of vendors of Windows-based accessibility utilities, refer to the following Web site: www.microsoft.com/enable/at/matvplist.aspx
---------------------	--

Quick Quiz 2

1. The VM Manager uses a(n) _____ replacement policy.
 - a. LRU
 - b. MRU
 - c. FCFS
 - d. FIFOAnswer: d

2. A(n) _____ is a data structure that controls how the I/O operation is processed at each step.
Answer: I/O request packet (IRP)
3. The segment of system memory labeled _____ is never paged to disk because it's used to store critical NT objects.
Answer: nonpaged pool

Class Discussion Topics

1. Have students discuss device management in Windows operating systems. How is it different from device management in the MS-DOS operating system? Ask students to list all the advanced key features of device management in Windows operating systems.
2. Have students discuss their thoughts on security management in Windows network operating systems? How do they feel about Microsoft's commitment to security?

Additional Projects

1. Have students research online to compile a list of the features of the Windows XP operating system that are designed to ensure Microsoft's design goals of compatibility and portability.
2. Ask students to describe two types of file I/O synchronization: synchronous file I/O and asynchronous file I/O. What are the pros and cons of each type? Provide examples of different situations in which each type would be suitable.

Additional Resources

1. Microsoft.com:
www.microsoft.com
2. Microsoft Windows:
www.microsoft.com/windows/default.mspx
3. MSDN Library:
<http://msdn.microsoft.com/library/>
4. Microsoft Security Guidance Kit:
www.microsoft.com/security/guidance

5. WindowSecurity.com:
www.windowsecurity.com

Key Terms

- **Active Directory:** Microsoft Windows directory service that offers centralized administration of application serving, authentication, and user registration for distributed networking systems.
- **Cache manager:** a component of the I/O system that manages the part of virtual memory known as cache. The cache expands or shrinks dynamically depending on the amount of memory available.
- **Compatibility:** the ability of an operating system to execute programs written for other operating systems or for earlier versions of the same system.
- **Domain Name Service or Domain Name System (DNS):** a general-purpose, distributed, replicated, data query service. Its principal function is the resolution of Internet addresses based on fully qualified domain names such as .com (for commercial entity) or .edu (for educational institution).
- **Extensibility:** one of an operating system's design goals that allows it to be easily enhanced as market requirements change.
- **Fetch policy:** the rules used by the Virtual Memory Manager to determine when a page is copied from disk to memory.
- **Graphical user interface (GUI):** a user interface that allows the user to activate operating system commands by clicking on desktop icons or menus using a pointing device such as a mouse or touch screen. GUI evolved from command-driven user interfaces.
- **Kerberos:** MIT-developed authentication system that allows network managers to administer and manage user authentication at the network level.
- **Kernel mode:** name given to indicate that processes are granted privileged access to the processor. Therefore, all machine instructions are allowed and system memory is accessible. Contrasts with the more restrictive user mode.
- **Lightweight Directory Access Protocol (LDAP):** a protocol that defines a method for creating searchable directories of resources on a network. It's called "lightweight" because it is a simplified and TCP/IP-enabled version of the X.500 directory protocol.
- **Mailslots:** a high-level network software interface for passing data among processes in a one-to-many and many-to-one communication mechanism. Mailslots are useful for broadcasting messages to any number of processes.
- **Named pipes:** a high-level software interface to NetBIOS, which represents the hardware in network applications as abstract objects. Named pipes are represented as file objects in Windows NT and later, and they operate under the same security mechanisms as other executive objects.
- **NT file system (NTFS):** the file system introduced with Windows NT that offers file management services, such as permission management, compression, transaction logs, and the ability to create a single volume spanning two or more physical disks.
- **Placement policy:** the rules used by the Virtual Memory Manager to determine where the virtual page is to be loaded in memory.
- **Portability:** the ability to move an entire operating system to a machine based on a different processor or configuration with as little recoding as possible.

- **POSIX:** Portable Operating System Interface, an operating system application program interface developed by the IEEE to increase the portability of application software.
- **Reliability:** the ability of an operating system to respond predictably to error conditions, even those caused by hardware failures; or the ability of an operating system to actively protect itself and its users from accidental or deliberate damage by user programs.
- **Replacement policy:** the rules used by the Virtual Memory Manager to determine which virtual page must be removed from memory to make room for a new page.
- **Ticket granting ticket:** a virtual “ticket” given by a Kerberos server indicating that the user holding the ticket can be granted access to specific applications servers. The user sends this encrypted ticket to the remote applications server, which can then examine it to verify the user’s identity and authenticate the user.
- **User mode:** name given to indicate that processes are not granted privileged access to the processor. Therefore, certain instructions are not allowed and system memory isn’t accessible. Contrasts with the less restrictive kernel mode.